COHESITY

WHITEPAPER

Moderne Topologien für Datensicherheit und -management: Ein Leitfaden für IT-Führungskräfte

Blueprints und Best Practices zur Risikominderung und Stärkung der Ausfallsicherheit von Unternehmen

INHALTSVERZEICHNIS

Einleitung

Drei Faktoren machen einen neuen Ansatz für Datensicherheit und -management erforderlich. Erstens: Die Notwendigkeit der digitalen Transformation und einer API-gesteuerten Infrastruktur. IT-Führungskräfte modernisieren jeden Aspekt ihrer IT-Infrastruktur, um Automatisierung, Erweiterbarkeit, Cloud-Skalierung, softwaredefinierte Architekturen und „Shift-Left"-Sicherheitsprinzipien stärker zu unterstützen.

Zweitens: Die Cyberbedrohungslandschaft entwickelt sich auf komplexe, unvorhersehbare Weise weiter. Die bestehenden Datenbestände vieler Unternehmen sind abgeschottet, was das operative Risiko eines Cyberangriffs erhöht. Einer aktuellen Umfrage zufolge sind 32 % der Unternehmen der Meinung, dass schnelle Wiederherstellungszeiten durch veraltete Systeme zur Datensicherung und -wiederherstellung beeinträchtigt werden. Ebenso geben 34 % an, dass auch eine mangelnde Integration zwischen IT- und Sicherheitsteams die Wiederherstellungszeiten verlängert.

Und drittens hat das Aufkommen von KI Führungskräfte dazu veranlasst, sich nach modernen Datenplattformen umzusehen, die Unternehmensdaten für generative KI-Technologien zugänglich machen.

Alle IT-Führungskräfte, die ein Datenmodernisierungsprojekt leiten, können davon profitieren, „auf den Schultern von Giganten zu stehen". In diesem Whitepaper beschreiben wir die wichtigsten Designüberlegungen und wie angesichts gängiger Unternehmensanforderungen der beste Ansatz für Datenresilienz gefunden werden kann. Unsere Erfahrungen aus Tausenden von Implementierungen und unser Wissen über Best Practices haben unsere Perspektiven geprägt.

Die folgenden Hinweise sind anbieterunabhängig, wir verwenden der Einfachheit halber jedoch die Markennamen von Cohesity.

Wichtige Designfaktoren

Jedes sinnvolle Modernisierungsprojekt birgt Risiken. Dies gilt natürlich auch für die Umgestaltung der Prozesse und Tools für Data Security and Data Management in Unternehmen. Doch die gute Nachricht ist: Sie können auf der Arbeit anderer aufbauen. Viele Unternehmen haben ihren Datenbestand erfolgreich modernisiert, und wir haben die Best Practices in diesem Dokument katalogisiert.

IT- und Cybersicherheitsverantwortliche stehen vor der Aufgabe, Agilität, Risiken und Kosten in ihrer gesamten IT-Infrastruktur in Einklang zu bringen. Diese Infrastruktur ist dynamisch und umfasst mittlerweile Daten und Anwendungen, die in lokalen Rechenzentren, Public Clouds, Colocation-Einrichtungen und Edge-Standorten ausgeführt werden. Modernisierungsbemühungen nehmen mit der Zeit an Skalierung und Ausmaß zu, da die schiere Menge der Anwendungen, Daten und Datenquellen wächst.

Die Modernisierung des Unternehmensdatenbestands wird zusätzlich erschwert durch:

- Unterschiedliche Infrastrukturziele an verschiedenen Standorten und mehrere Workloads, was zu Datenfragmentierung und ineffizienten Datensicherungs- und -wiederherstellungsprozessen führt
- Mangelnde IT- und Cybersicherheitskompetenz in den meisten Unternehmen
- Eine sich rasant verändernde Cybersicherheitslandschaft mit Hunderten von Angriffen pro Minute. Angesichts der Entwicklung und Raffinesse der Angriffe ist eine frühzeitige Erkennung von entscheidender Bedeutung.

Dennoch gibt es einige „Grundprinzipien“, die Sie beachten sollten.

Die 3:2:1-Regel gilt weiterhin

Die 3:2:1-Regel besagt, dass mindestens drei Kopien der Daten aufbewahrt werden sollten, diese Backups auf zwei verschiedenen Medien oder Plattformen gespeichert werden sollten und mindestens eine der Kopien standortfern aufbewahrt werden sollte.

Der nachhaltige Wert der 3:2:1-Regel beruht auf drei Konzepten, die auch im cloudnativen Zeitalter die Gestaltung der Systemtopologie prägen:

- Geschäftsanforderungen
- Fehlerdomänen
- Höhere Gewalt

Wir werden jedes dieser Konzepte im Detail beschreiben. Sie waren schon immer ein Schwerpunkt der Branche und sind es auch heute noch – insbesondere angesichts der zunehmenden Bedenken hinsichtlich Cyberangriffen. Cyberangriffe standen nicht immer im Mittelpunkt, heute allerdings ganz eindeutig.

Wir erläutern zum einen, wie diese drei Konzepte im Laufe der Zeit die Datensicherungs- und -wiederherstellungsdesigns beeinflusst haben. Außerdem erörtern wir, wie die Sorge um Cyberangriffe unsere Kunden dazu zwingt, sich zu fragen, ob ihre bestehenden Bereitstellungstopologien noch ausreichen (oder nicht).

Lassen Sie uns die Punkte einzeln durchgehen:

Geschäftsanforderungen

Unternehmen müssen eine Vielzahl geschäftlicher, gesetzlicher und Compliance-Anforderungen erfüllen. Viele dieser Anforderungen erfordern die Aufbewahrung aktueller und älterer Daten. Es könnte beispielsweise sein, dass ein Compliance-Team einen drei Jahre alten Vertrag abrufen muss, um der Anfrage einer Branchenaufsichtsbehörde nachzukommen. Es kann auch vorkommen, dass ein Steuerteam Dateien für einen laufenden Audit wiederherstellen muss. Oder, um ein anschaulicheres Beispiel zu nennen: Vielleicht wurde eine wichtige Datei versehentlich gelöscht und muss wiederhergestellt werden.

Fehlerdomänen

In der IT-Branche ist bekannt, dass sowohl Software als auch Hardware ausfallen können. Hard- und Softwareanbieter unternehmen enorme Anstrengungen, um diese Unvermeidlichkeit zu umgehen, aber dennoch kommt es immer wieder zu Ausfällen. IT-Teams müssen Ausfälle einplanen und sicherstellen, dass diese keine negativen Auswirkungen auf das Unternehmen oder das Geschäft haben. Beispiele für Ausfälle sind Workload-Probleme wie etwa die Beschädigung von VMs oder Speichervolumes, oder die fehlgeschlagene Implementierung eines Betriebssystem-Patches. In beiden Fällen muss das IT-Team den Fehler beheben und benötigt dafür wahrscheinlich Daten aus seinem Datensicherungs- und -wiederherstellungssystem.

Vor Jahrzehnten mussten sich Führungskräfte keine Sorgen über Ausfälle durch böswillige Akteure machen. Heute sind Cyberangriffe nicht nur eine Hauptursache für Systemausfälle, sondern möglicherweise die sichtbarste Fehlerursache – und eine, die die Aufmerksamkeit des Vorstands auf sich zieht.

Höhere Gewalt

Dieser Begriff bezieht sich auf Naturkatastrophen oder andere Ereignisse, die außerhalb menschlicher Kontrolle liegen und mit angemessenen Mitteln nicht vorhergesehen oder verhindert werden können. Unerwünschte Ereignisse wie Brände, Erdbeben, Überschwemmungen und Kabelbrüche gelten als „höhere Gewalt“. Wie bei Fehlerdomänen müssen IT-Unternehmen das Potenzial für höhere Gewalt berücksichtigen und entsprechend ausfallsichere Systeme entwickeln.

Die 3:2:1-Regel bietet praktische Hilfestellung für den Umgang mit
höherer Gewalt.

Da Systeme ausfallen, ist es sinnvoll, mehrere Kopien der Daten bereitzuhalten. Aufgrund von Fehlerdomänen ist es zudem ratsam, Backups auf zwei verschiedenen Medientypen oder Systemen aufzubewahren. Schließlich zeugt es von verantwortungsvoller Unternehmensführung, bei höherer Gewalt mindestens eine dieser Kopien an einem entfernten Standort aufzubewahren, beispielsweise als Teil eines Disaster Recovery-Standorts oder eines entfernten Rechenzentrums.

Selbst bei unterschiedlichen Anforderungen gibt es Gemeinsamkeiten

Obwohl die 3:2:1-Regel eine bewährte Praxis ist, entscheiden sich Unternehmen möglicherweise für Bereitstellungen mit weniger als drei Kopien. Andere halten sich strikter an die 3:2:1-Regel. Wieder andere bewahren mehr als drei Kopien auf. (Die Gründe für diese Designentscheidungen werden wir später in diesem Dokument erläutern.)

Hinsichtlich des Designs haben wir die Bereitstellungstopologien („Blueprints“) in drei Typen gruppiert.

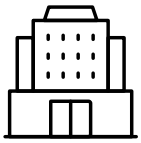
Typ	Beschreibung
Basic-Topologien	Eine Bereitstellungstopologie mit zwei oder weniger Kopien
Erweitert	Eine Bereitstellungstopologie mit drei Kopien
Aufgabenkritisch	Eine Bereitstellungstopologie mit vier oder mehr Kopien

Bekannte Verfügbarkeitsarchitekturen sind auch heute noch relevant

Kommen wir zu einem Begriff, der erfahrenen IT-Führungskräften und -Praktikern geläufiger sein dürfte: Verfügbarkeitsarchitektur.

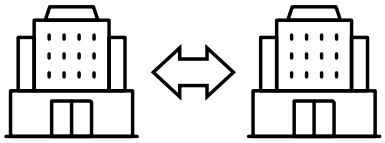
Eine Verfügbarkeitsarchitektur beschreibt, wie ein IT-Team seine Hard- und Softwaresysteme so organisiert, dass sie einem möglichen Ausfall standhalten. Unserer Erfahrung nach basieren die meisten Implementierungen in Unternehmen auf einer von drei Kundenverfügbarkeitsarchitekturen: ***Active-Active, Active-Standby und Hub-and-Spoke***.

Alle diese Ansätze werden im Folgenden vorgestellt.



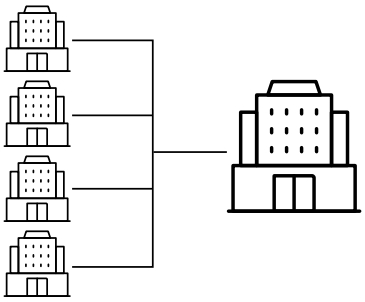
Aktiv-Standby

Die Workloads laufen über ein einziges Rechenzentrum. Häufig gibt es einen Standby-Standort für die Notfallwiederherstellung, der im Falle eines Ausfalls die Aufgaben übernimmt.



Aktiv-Aktiv

Die primären Workloads sind auf zwei Rechenzentren verteilt. Im Falle eines Ausfalls eines Rechenzentrums kann das verbleibende Rechenzentrum die gesamte Last übernehmen.



Naben- und Speichenmodell

Die Workloads zeichnen sich durch eine große Anzahl von Remote-/Zweigstellen aus, die mit einem einzigen Rechenzentrum verbunden sind.

Abb. 1: Kundenverfügbarkeitsarchitekturen

In jedem Fall soll die Verfügbarkeitsarchitektur sicherstellen, dass der Geschäftsbetrieb bei einem Ausfall fortgesetzt werden kann. Fällt die „aktive" Seite einer **Active-Standby**-Architektur aus, wird die gesamte Verarbeitung auf das andere Standby-System umgeschaltet. Fällt eine Seite eines **Active-Active**-Systems aus, übernimmt die andere Seite 100 % des Workloads. Tritt ein Ausfall in einem **Hub-and-Spoke**-System auf, beispielsweise wenn Daten durch einen Hardwarefehler oder ein anderes Problem in einer Zweigstelle zerstört werden, können das System und seine Daten vom Hub wiederhergestellt werden, sobald die Fehlerursache behoben ist.

Verantwortliche IT-Teams haben diese Verfügbarkeitsarchitekturen entwickelt und testen sie regelmäßig, um zu gewährleisten, dass die Resilienzmechanismen ordnungsgemäß funktionieren.

Unsere gesammelten Best Practices an Blueprints basieren auf diesen bewährten Verfügbarkeitsarchitekturen. Bei Cohesity implementieren wir Datensicherungs- und -wiederherstellungssysteme nicht isoliert. Wir entwickeln sie so, dass sie eng mit der zugrunde liegenden IT-Infrastruktur harmonieren. Wir gehen später bei den verschiedenen Datensicherungs- und -wiederherstellungstopologien und deren Zuordnung zu IT-Verfügbarkeitsarchitekturen noch detaillierter darauf ein.

Blueprints für Data Security and Management von heute: Typen und Topologien

Wir haben bereits grundlegende, erweiterte und aufgabenkritische Sicherungstypen besprochen. Nun stellen wir Ihnen die mit diesen Typen verbundenen Topologien vor.

Zunächst jedoch einige Definitionen. Datensicherheits- und -managementsysteme können Daten auf unterschiedliche Weise speichern. Datenkopien können als Backups, Replikate oder Archive aufbewahrt werden.

Als Faustregeln gelten:

- **Backups** werden aus einer Primärkopie erstellt und führen zu deduplizierten, komprimierten und verschlüsselten Daten. Diese Verarbeitung wird einmalig durchgeführt. Anschließend können die verarbeiteten Backup-Daten in ein Replikat oder Archiv kopiert werden.
- **Replikate** dienen in der Regel der kurzfristigen Aufbewahrung, typischerweise für Monate, nicht aber für Jahre. Diese Replikate unterstützen häufig IT-Verfügbarkeitsarchitekturen wie Active-Active oder Active-Standby.
- **Archive** dienen im Allgemeinen der längerfristigen Aufbewahrung und werden oft jahrelang verwahrt. Sie werden häufig für Compliance- und Regulierungszwecke, manchmal aber auch für IT-Verfügbarkeitsarchitekturen eingesetzt.
- **Die Wiederherstellung aus einem Backup oder Replikat** erfolgt in einem Schritt und ist schneller als die Wiederherstellung aus einem Archiv, die ein zweistufiger Prozess ist. Das Archiv muss zunächst in das Backup- und Recovery-System des Anbieters heruntergeladen werden, bevor es im IT-System wiederhergestellt wird.
- **Die Recovery nach einem Ransomware-Angriff** wird dadurch erschwert, dass eine saubere, nicht infizierte Kopie wiederhergestellt werden muss, die vermutlich nicht die aktuellste Sicherung ist. Ein Unternehmen kann sich von einem Ransomware-Angriff nicht einfach auf die gleiche Weise erholen wie von einem Domänenausfall oder einer Unterbrechung, die durch höhere Gewalt verursacht wurde. Das betroffene Unternehmen muss die Umgebung analysieren und sicherstellen, dass die wiederhergestellten Kopien frei von der Malware-Infektion sind, die den Angriff ursprünglich verursacht hat.

Die Liste der Topologien finden Sie in der unten stehenden Tabelle. Beachten Sie, dass jede Topologie über ein einzelnes Backup verfügt, in dem die Daten dedupliziert, komprimiert und verschlüsselt sind. Zusätzlich zum Backup können die verschiedenen Topologien ein oder mehrere Replikate sowie ein oder mehrere Archive speichern. Um den Überblick zu behalten, haben wir jedem Topologietyp einen Deskriptor (B1, B2, E1, E2, M1, M2 usw.) zugewiesen.

Typ	Kopien	Topologie / Kopientyp
Basic-Topologien	1	B1 – Backup
	2	B2 – Backup und Archiv
	2	B3 – Backup und Replikation
Erweitert	3	E1 – Backup, Replikation und Archiv
	3	E2 – Backup und doppelte Replikation
Aufgaben-kritisch	4	M1 – Backup und doppelte Replikation mit Archiv
	4	M2 – Backup, Replikation und Doppelarchiv
	5	M3 – Backup, doppelte Replikation und Doppelarchiv

Eine Typ-Topologie-Kombination wird sowohl durch **die Anzahl der Kopien als auch durch deren Art definiert**. Beispielsweise kann ein erweiterter Typ, der immer drei Kopien umfasst, zwei unterschiedliche Topologien haben. Eine Topologie umfasst Backup, Replikation und Archiv, die andere Backup und doppelte Replikation. Beachten Sie, dass oben nicht jede Variante von Datenkopien aufgeführt ist; diese Liste stellt lediglich die gängigsten Bereitstellungen dar. Manche Kombinationen sind aus geschäftlicher oder technischer Sicht schlicht nicht sinnvoll.

Es ist hilfreich zu wissen, welche Topologien häufig verwendet werden und welche nicht. Die relative Beliebtheit der einzelnen Muster kann nützliche Anhaltspunkte für Upgrades bieten, wenn IT-Teams zusätzlichen Schutz für ihren Datenbestand in Betracht ziehen.

Blueprints: Die vollständige Liste der Topologien

Nachdem wir nun die Typen, Topologien und Architekturen der Kundenverfügbarkeit beschrieben haben, sehen wir uns nun die vollständige Liste der Branchenkonzepte an.

Dieses Diagramm fasst alle zuvor besprochenen Konzepte zusammen. Alle Konfigurationen sind in der Praxis beliebt, da Unternehmen Cohesity bereits in großem Maßstab einsetzen.

Typ	Topologie / Kopientyp	Kundenverfügbarkeitsarchitektur		
		Active-Standby	Active-Active	Hub-and-Spoke
Basic-Topologien	B1 Backup (1)	•	•	
	B2 Backup und Archiv (2)	•	•	
	B3 Backup und Replikation (2)	•	•	
Erweitert	E1 Backup, Replikation und Archiv (3)	•	• •	•
	E2 Backup und doppelte Replikation (3)	•	•	
Aufgaben-kritisch	M1 Backup und doppelte Replikation mit Archiv (4)	•		
	M2 Backup, Replikation und Doppelarchiv (4)	•	•	
	M3 Backup, doppelte Replikation und Doppelarchiv (5)		•	

Es gibt einen Vorbehalt zu den aufgabenkritischen Topologien. Diese Topologien wurden bereits bei Unternehmen oder anderen Großkunden implementiert, demonstriert, getestet oder ausführlich diskutiert. Wir haben zuvor festgestellt, dass viele Kunden eine höhere Ausfallsicherheit ihrer Implementierungen wünschen. Die Diskussionen drehen sich um praktische Möglichkeiten zum Schutz zusätzlicher Datenkopien. Eine gängige Lösung ist die Erweiterung der Implementierung mit einem Datentresor. Aus diesem Grund enthalten viele aufgabenkritische Topologien ein als Datentresor konfiguriertes Archiv. (Für dieses Szenario bieten wir Cohesity FortKnox an.) Viele Topologien können durch die Erweiterung eines Datentresors cyber-resilienter gemacht werden.

Wir besprechen jetzt die Typen und Topologien im Detail, eine Gruppe nach der anderen.

Basic-Topologien

Topologie	Primäres Rechenzentrum	Active-Active
B1 – Backup	✓	✓
B2 – Backup und Archiv	✓	✓
B3 – Backup und Replikation	✓	✓

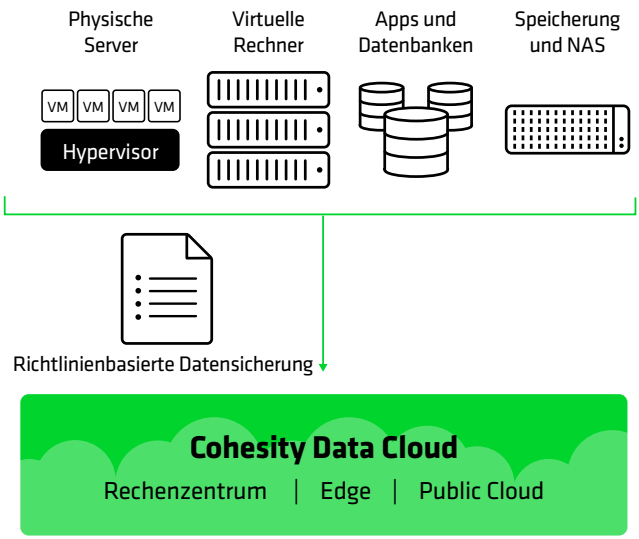
Die Basic-Topologie eignet sich für Daten mit geringem und mittlerem Wert oder wenn der Kunde bereits mehrere Kopien seiner Daten besitzt. Basic-Topologien werden bei einem einzelnen, primären Rechenzentrum sowie bei Active-Active-Ansätzen eingesetzt.

Was ist ein Datentresor?

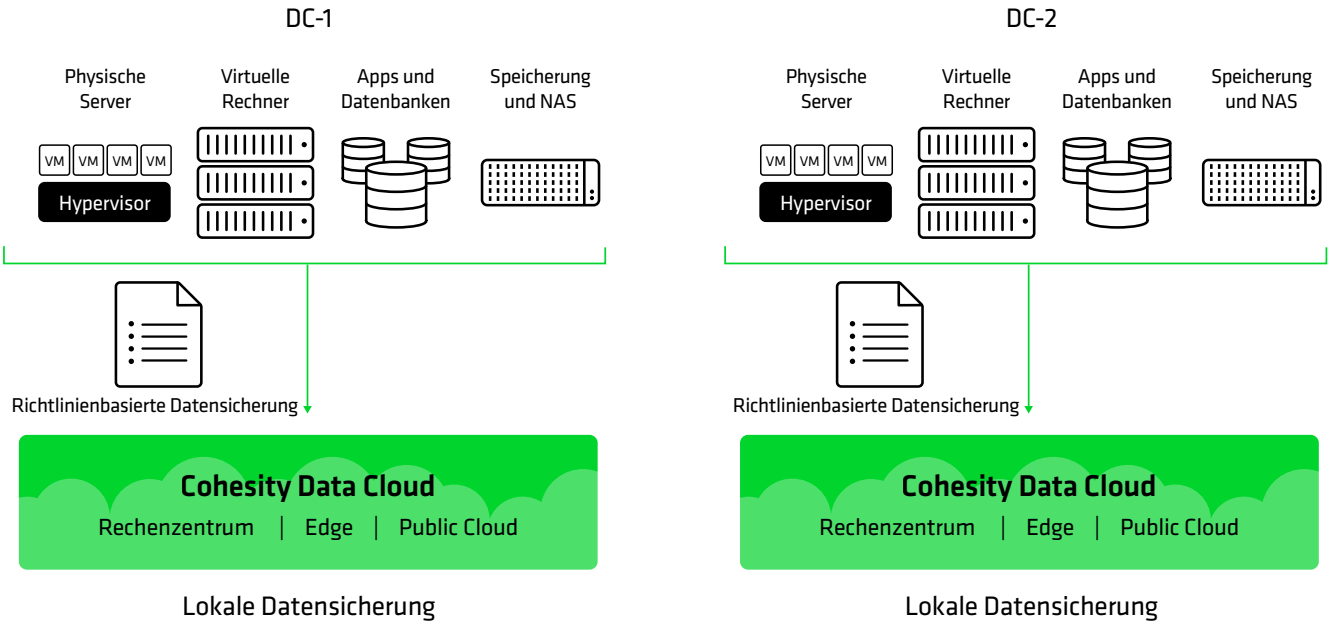
In einem Datentresor wird eine isolierte Kopie der Produktionsdaten gespeichert, oft außerhalb des Standorts. Unternehmen besitzen so eine saubere, separate und geschützte Kopie ihrer Daten, die immer verfügbar ist. Im Fall eines Ransomware-Angriffs oder eines anderen Vorfalls, der die Produktion oder die primären Backup-Systeme gefährdet, können sie die Daten schnell wieder an der ursprünglichen Quelle oder an alternativen Backup-Speicherorten wiederherstellen. Moderne Cyber-Tresor-Strategien nutzen ein „Virtual Air Gap“-Konzept. Diese Technologie schützt Backups, lässt aber temporäre Netzwerkverbindungen zu, um den notwendigen Fernzugriff zu ermöglichen – allerdings mit sehr strengen Kontrollen. Gleichzeitig werden die Daten bei Bedarf weiter von der Cloud isoliert. Ein sorgfältig konzipierter Cyber-Tresor kann eine robuste Strategie zur Datenisolation und Cyber-Resilienz effektiv unterstützen.

Basic: B1 – Lokales Backup

Dies ist ein sehr vereinfachter Ansatz mit nur einer zentralen Sicherungskopie der Daten. Viele IT-Rechenzentren nutzen diesen Ansatz nach wie vor, obwohl er weder eine Notfallwiederherstellung noch eine langfristige Aufbewahrung der Backup-Daten vorsieht. Dieser Ansatz wird typischerweise für Daten mit geringem Wert verwendet.



Basic: B1 – Backup (Active-Active)

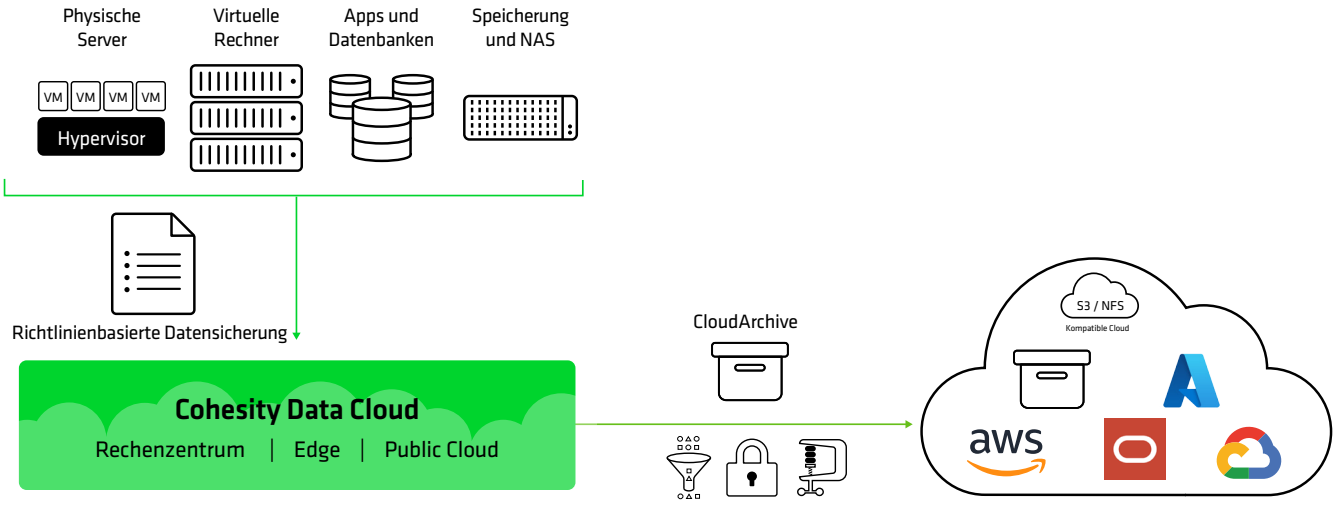


Lokale Datensicherung

Lokale Datensicherung

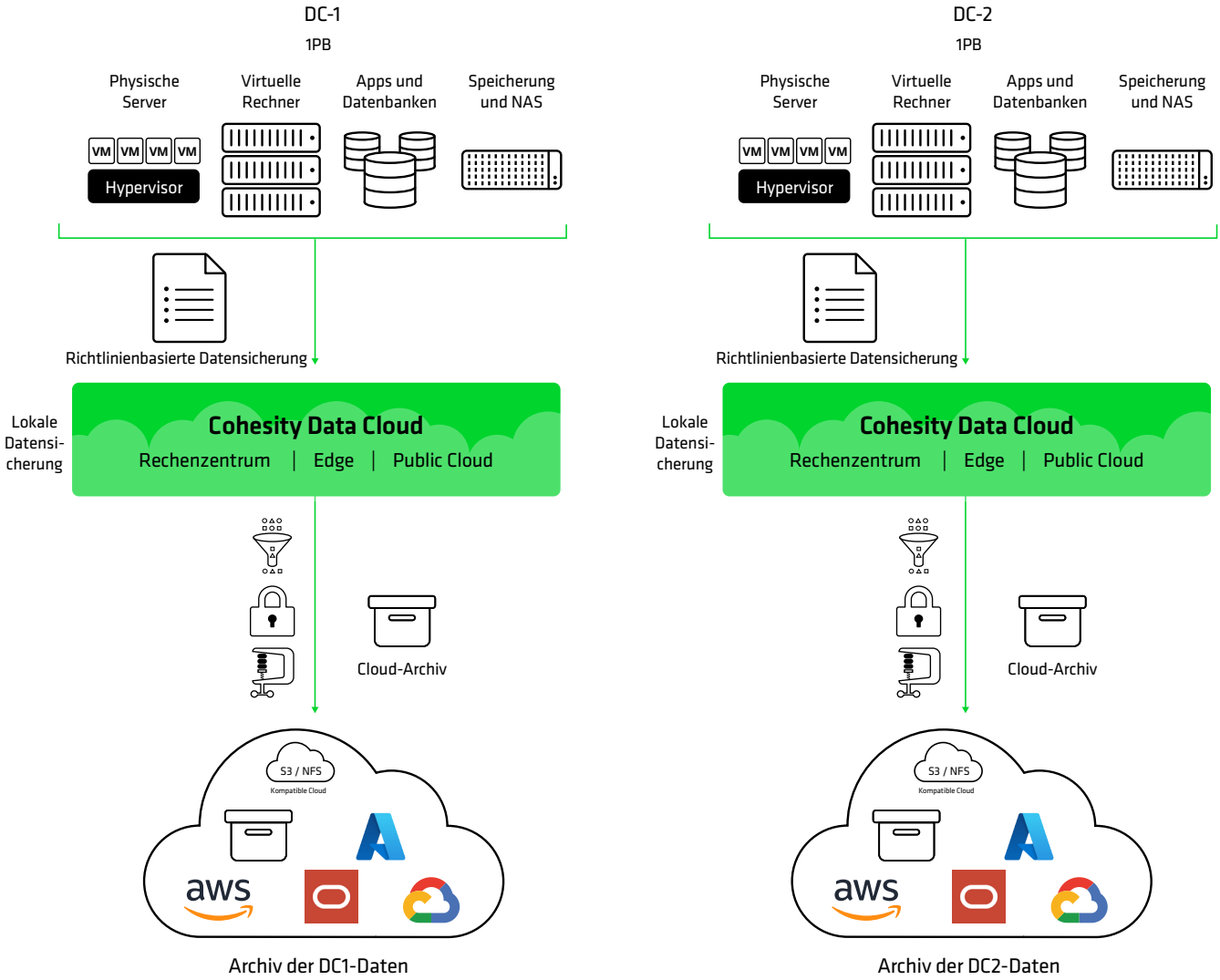
Viele Typen und Topologien eignen sich für einen Active-Active-Ansatz. Dieser Ansatz besteht im Prinzip aus zwei Topologien eines Typs, gespiegelt und Back-to-Back. In dieser Topologie gibt es zwei Active-Active-Rechenzentren mit jeweils eigenem Backup. Bei einem Ausfall kann jedes Rechenzentrum das andere übernehmen. Jedes Rechenzentrum verfügt zudem über ein vollständiges Backup seiner Daten und Workloads. Für Kunden mit großer verfügbarer WAN-Bandbreite kann sogar das Backup geografisch vom Rechenzentrum getrennt werden, um zusätzlichen Katastrophenschutz zu gewährleisten. Die gesamte Replikation von Workloads und Daten erfolgt auf der Workload-Ebene, daher ist in dieser Topologie keine Replikation erforderlich.

Basic: B2 – Backup und Archiv



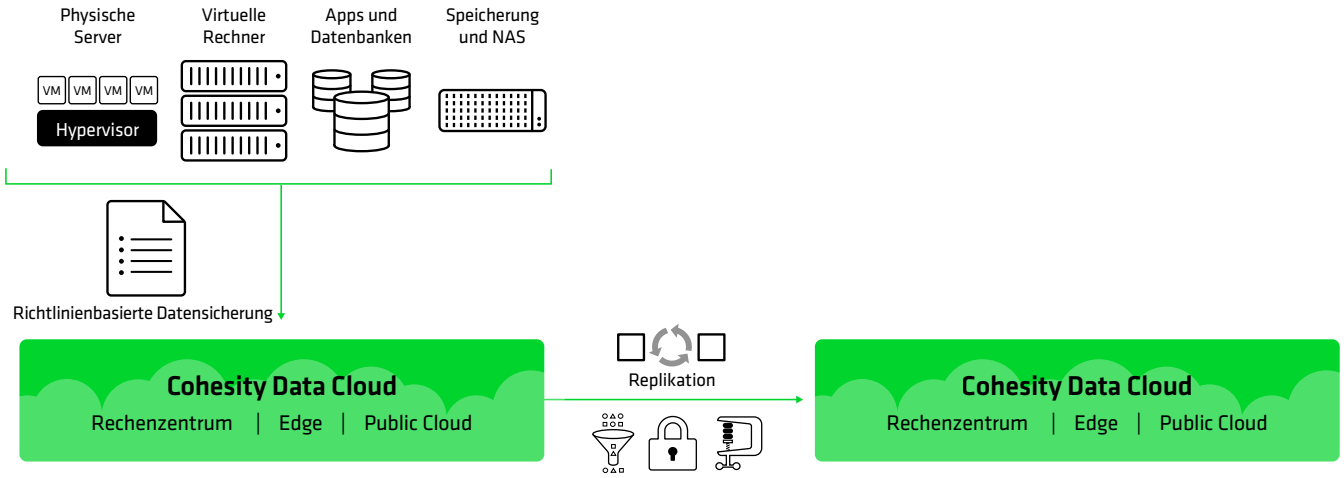
In diesem Fall wird das Backup mit einem Archiv gekoppelt, dessen Aufbewahrungsdauer deutlich länger ist als die eines Backups. Cohesity FortKnox ist hier eine beliebte Wahl, da es zusätzliche Sicherheit für diese Topologie bietet. FortKnox ist ein isoliertes Archiv und wird nur verbunden, wenn ein Schreibvorgang in das Archiv oder eine Wiederherstellung aus dem Archiv erfolgt. Das Archiv kann auch in einer lokalen/externen Private Cloud oder einer Public Cloud wie AWS, Google Cloud, Microsoft Azure, Oracle Cloud oder einem beliebigen S3/NFS-kompatiblen Cloud-Dienst gespeichert werden.

Basic: B2 – Backup und Archiv (Active-Active)



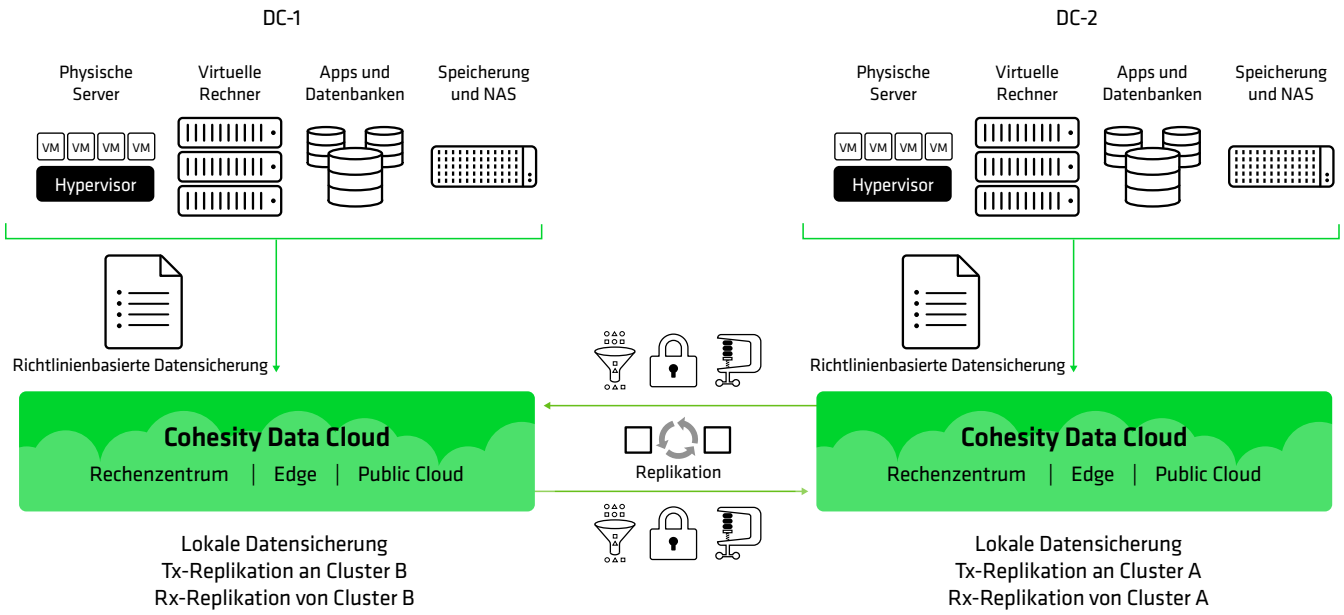
In dieser Topologie verfügen wir über zwei Active-Active-Rechenzentren mit jeweils eigenem Backup und Archiv. Jedes Rechenzentrum kann im Falle eines Ausfalls die Aufgaben des anderen übernehmen, und jedes Rechenzentrum verfügt über ein vollständiges Backup seiner Daten und Workloads durch das Archiv. Die gesamte Replikation von Workloads und Daten erfolgt auf der Workload-Ebene, daher ist in dieser Topologie keine Replikation erforderlich. FortKnox wäre aufgrund seiner Isolation und zusätzlichen Sicherheit eine sinnvolle Wahl für das Archiv.

Basic: B3 – Backup und Replikation (Disaster Recovery)



In dieser Topologie sind Backup und Replikat hinsichtlich der Aufbewahrungsdauer grob aufeinander abgestimmt. Das Replikat ist geografisch verteilt und dient der Wiederherstellung im Notfall. Für Kunden mit großer verfügbarer WAN-Bandbreite kann sogar das Backup geografisch vom Rechenzentrum getrennt werden, um zusätzlichen Katastrophenschutz zu gewährleisten. Der Schwerpunkt dieser Topologie liegt auf der Geschäftskontinuität, falls das Backup nicht verfügbar ist. Replikate können Daten direkt wiederherstellen, ohne dass der zweistufige Prozess durchlaufen werden muss, der bei der Verwendung eines Archivs erforderlich ist.

Basic: B3 – Backup und Cross-Replikation (Active-Active)



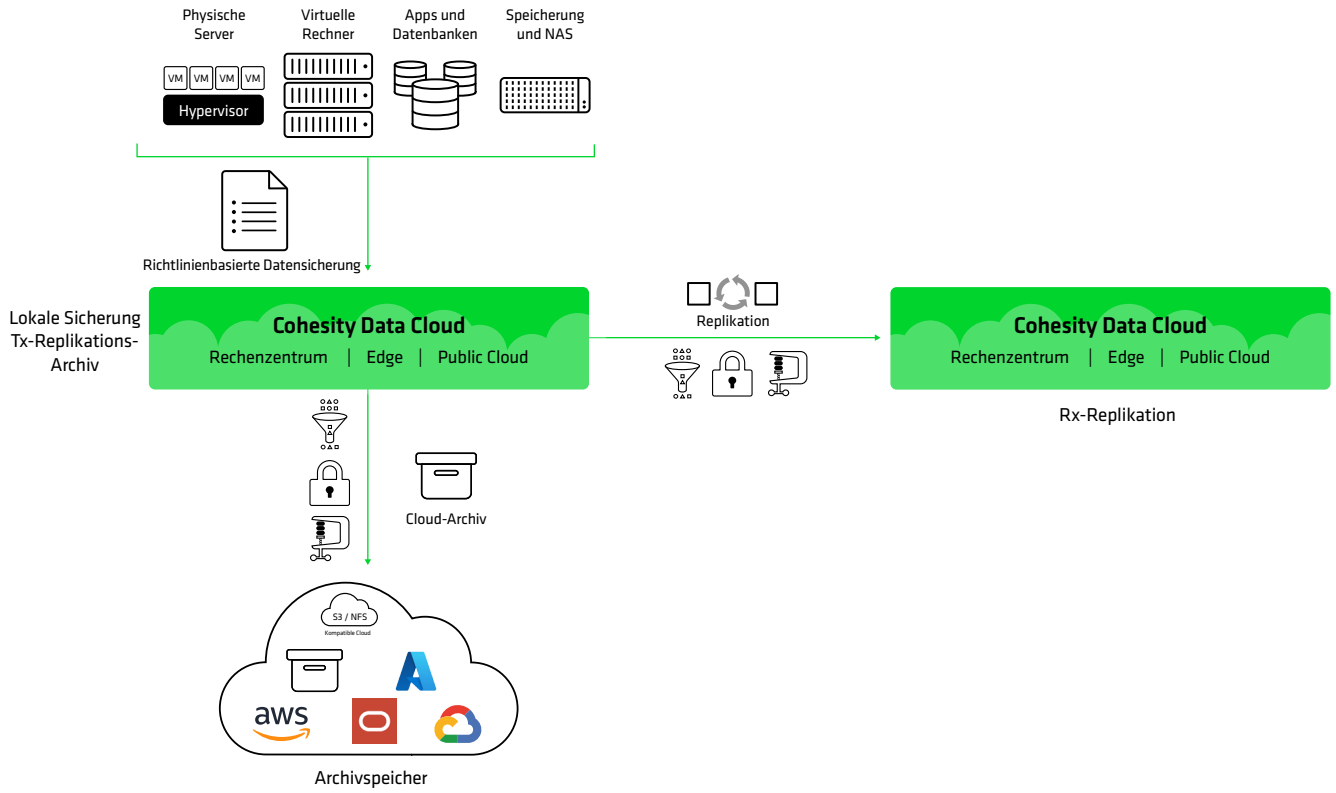
In diesem Fall werden Backup- und Replikations-Cluster kreuzweise repliziert. Das Backup für den ersten Standort ist das Replikat für den zweiten Standort und umgekehrt.

Erweiterte Topologien (einschließlich der Übernahme durch die Industrie)

Erweiterte Topologien sind bei wertvollen Daten weit verbreitet. Backup, Replikation und Archiv (E1) ist am beliebtesten, Backup und doppelte Replikation (E2) hingegen weniger. Die gängigsten Topologien sind unten aufgeführt, zusammen mit bemerkenswerten Favoriten der Industrie.

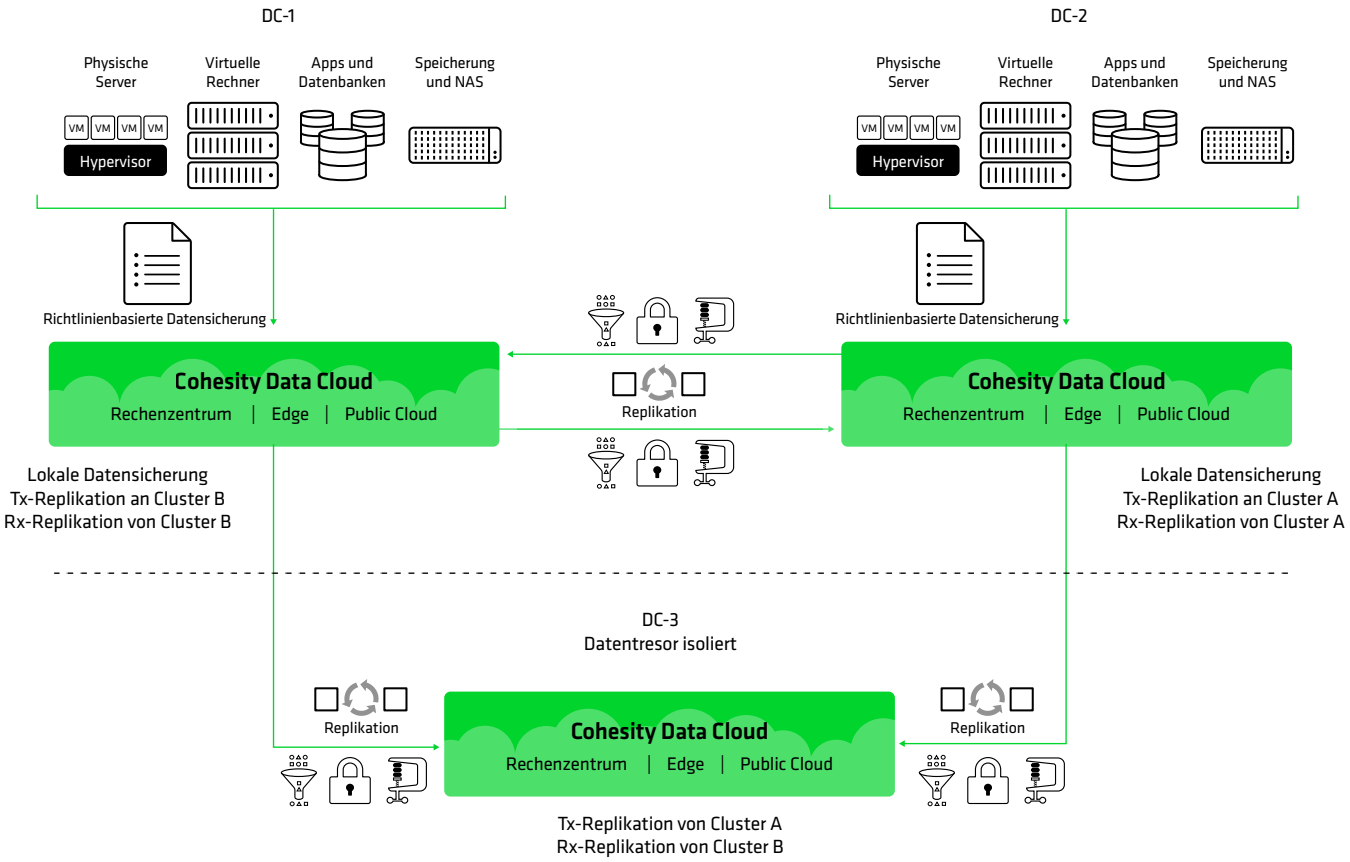
Topologie	Primäres Rechenzentrum	Active-Active	Hub-and-Spoke
E1 – Backup, Replikation und Archiv	✓ Alle Typen	✓ Finanz-institute	
E2 – Backup und doppelte Replikation	✓ Staatliche Behörden	✓ Einzelhandelsketten und einige staatliche Behörden verwenden ein Ost-West-Modell	

Erweitert: E1 – Backup, Replikation und Archiv



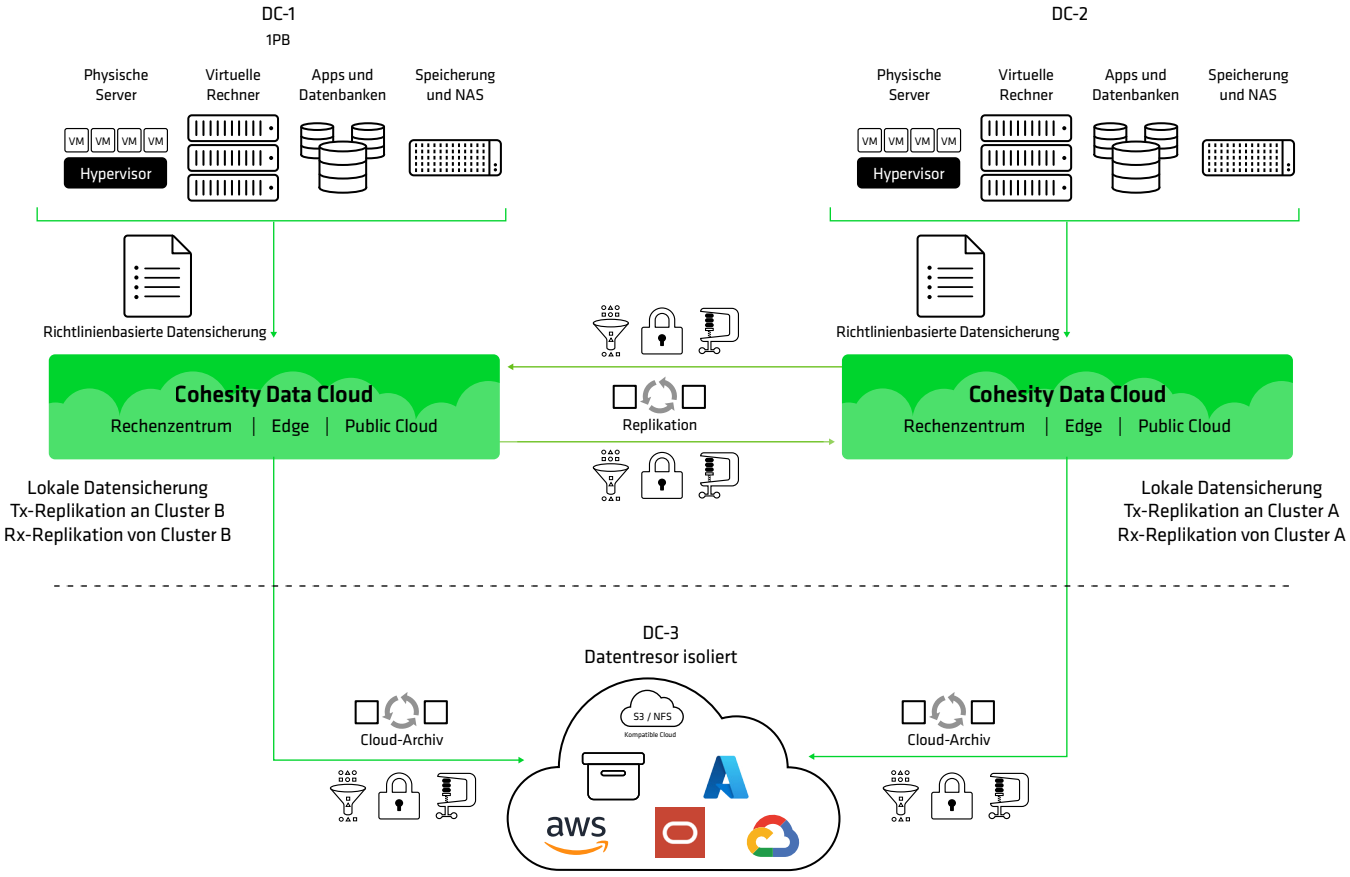
Backup und Replikat sind grob aufeinander abgestimmt (z. B. zweimal täglich für 90 Tage), während das Archiv Monate oder sogar Jahre umfassen kann. Die Wiederherstellung aus einem Backup oder Replikat erfolgt in einem Schritt, während die Wiederherstellung aus einem Archiv zwei Schritte umfasst: Lesen des Archivs und anschließendes Wiederherstellen der Daten. Das Archiv kann in einer lokalen/externen Private Cloud oder in einer Public Cloud wie AWS, Google Cloud, Microsoft Azure, Oracle Cloud oder einem beliebigen S3/NFS-kompatiblen Cloud-Dienst gespeichert werden. FortKnox eignet sich aufgrund seiner zusätzlichen Isolation und Sicherheit ebenfalls hervorragend für diese Topologie. Beachten Sie, dass mit der Cohesity Data Cloud ein Archiv entweder über einen primären oder sekundären Cluster wiederhergestellt werden kann.

Erweitert: E1 – Active-Active mit einem Datentresor



Diese Topologie ist ein weiterer **Active-Active**-Ansatz. Hier teilen sich die kreuzreplizierten Rechenzentren einen isolierten Datentresor. Die Isolation erfolgt physisch, wobei der Datentresor bei Nichtgebrauch vom Netzwerk getrennt wird. Beachten Sie, dass es sich bei dem Tresor um ein Replikat handelt, das eine einstufige Wiederherstellung beider Rechenzentren vom Replikat aus ermöglicht. Diese Architektur lässt sich auch erweitern, indem mehrere Active-Active-Paare denselben Datentresor nutzen.

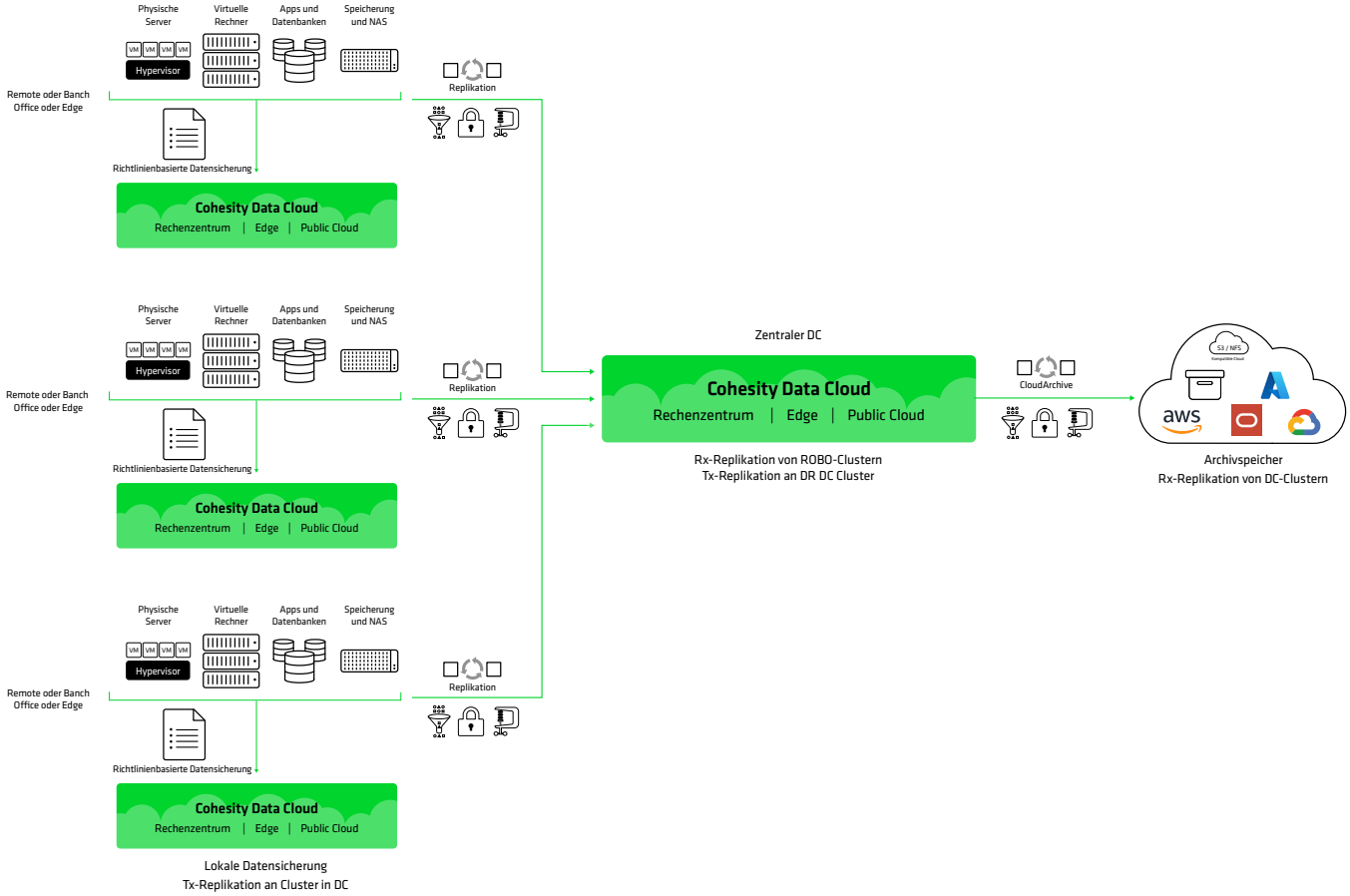
Erweitert: E1 – Active-Active mit einem isolierten Archiv



Die obige Grafik zeigt einen weiteren **Active-Active-**Ansatz. In diesem Fall nutzen die kreuzreplizierten Rechenzentren ein isoliertes Archiv. Dieser Anwendungsfall würde aufgrund seiner Isolation und zusätzlichen Sicherheit gut mit unserem FortKnox-Archivierungsansatz funktionieren.

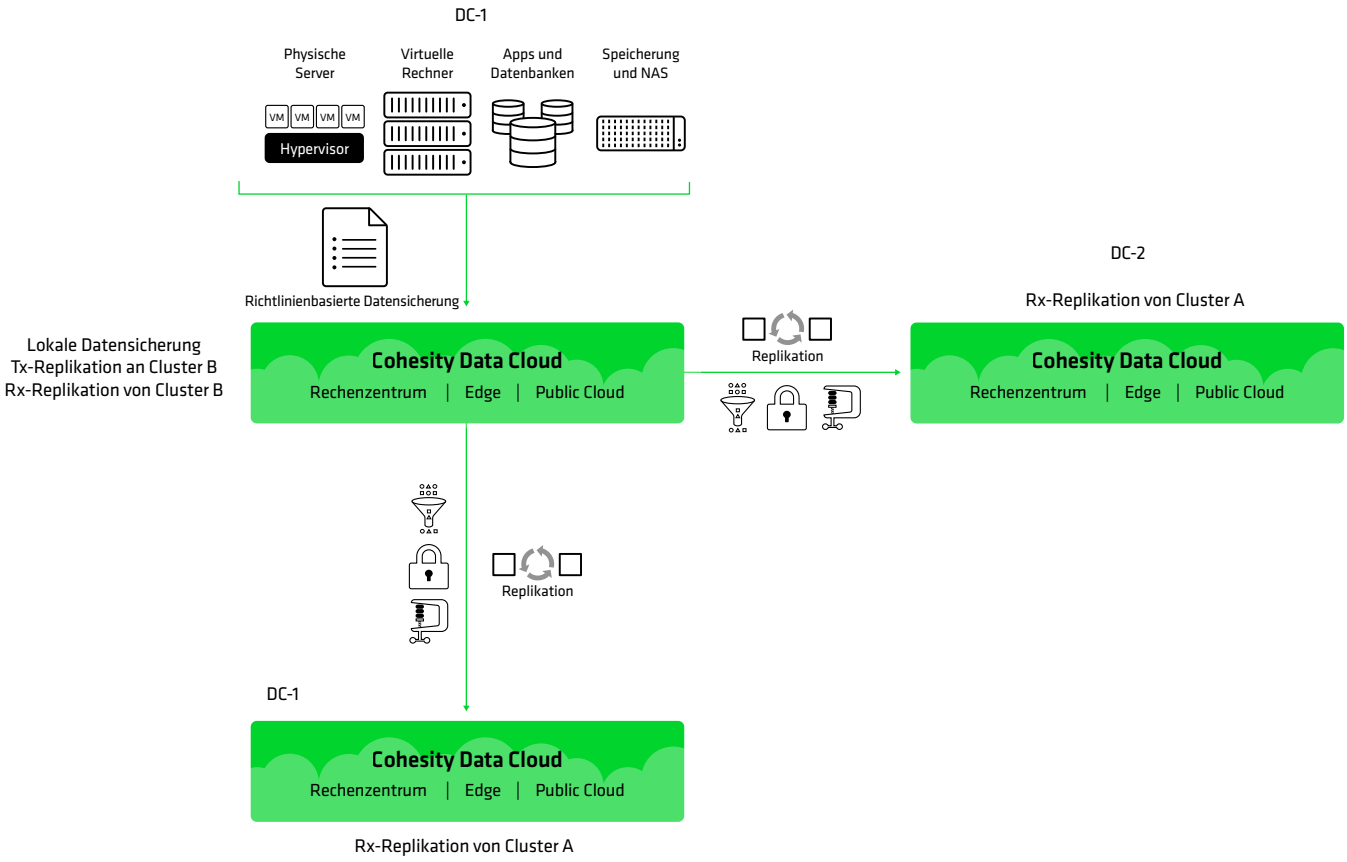
Diese Architektur lässt sich auch erweitern, indem mehrere Active-Active-Paare dasselbe isolierte Archiv verwenden. Mit der Cohesity Data Cloud kann ein Archiv in jedem Backup oder Replikat wiederhergestellt werden.

Erweitert: E1 – Backup, Replikation und Archiv (Hub-and-Spoke)



Viele Topologien lassen sich auch auf **Hub-and-Spoke**-Modelle erweitern, die auch als Fan-In-Topologie bezeichnet werden. Im Hub-and-Spoke-Modell verfügen einzelne Zweigstellen über eigene Backups, die in eine einzige integrierte Cohesity Data Cloud in einem zentralen Rechenzentrum repliziert werden. Vom zentralen Rechenzentrum aus wird das Replikat über FortKnox oder in einem anderen privaten oder öffentlichen Archiv archiviert. FortKnox bietet sich hierfür an, da es im Falle einer Kompromittierung sowohl der Backups als auch des Replikats vollständige Isolation bietet. Mit der Cohesity Data Cloud kann ein Archiv über einen primären oder sekundären Cluster wiederhergestellt werden.

Erweitert: E2 – Backup und doppelte Replikation



Diese Topologie eignet sich für Fälle, in denen der zweistufige Wiederherstellungsprozess aus einem Archiv keine ausreichend niedrige RTO bietet. Bei dieser Konfiguration können alle drei Kopien (das Backup und beide Replikate) verwendet werden, um die Daten in einem einstufigen Prozess wiederherzustellen.

Erweitert: E2 – Hub-and-Spoke mit Active-Active-Hubs

Diese Topologie kombiniert mehrere verschiedene Modelle. Die Zweigstellen erstellen jeweils eigene Backups, die in einem zentralen Rechenzentrum repliziert werden. Dieses zentrale Rechenzentrum verfügt zudem über ein Disaster Recovery-Rechenzentrum als Backup. Dies alles wird gespiegelt, wobei das primäre Rechenzentrum links als Disaster Recovery-Standort für das rechte Rechenzentrum dient und umgekehrt.

Aufgabenkritische Topologien

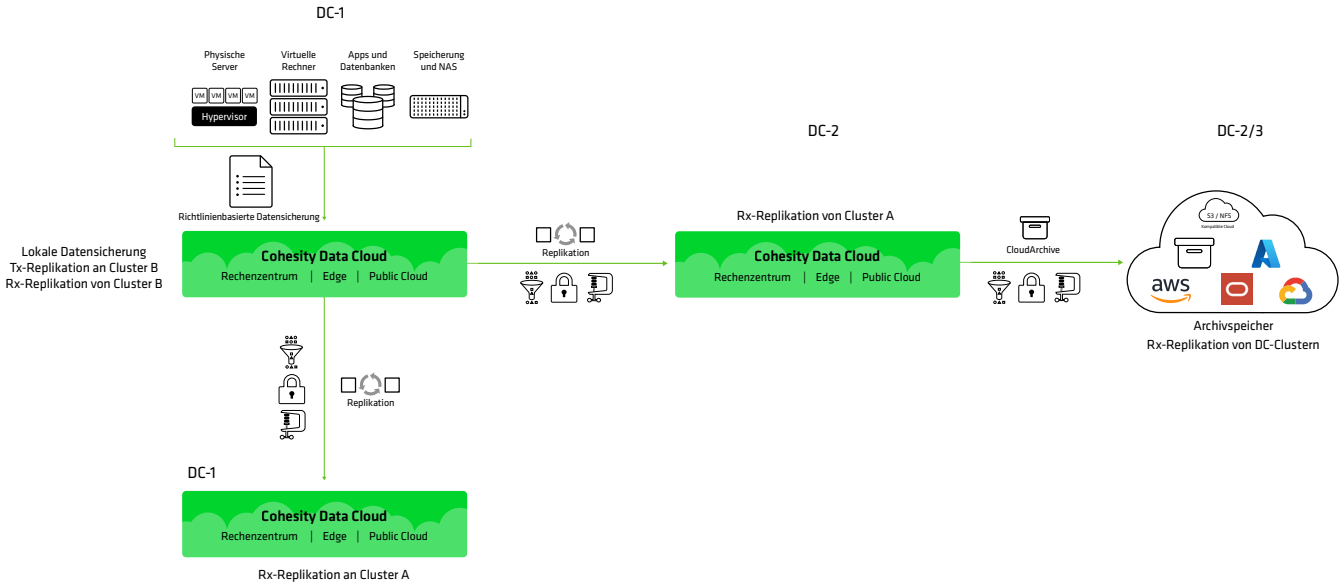
Topologie	Zentrales Rechenzentrum	Active-Active	Hub-and-Spoke
Backup und doppelte Replikation mit Archiv	✓		✓
Backup, Replikation und Doppelarchiv	✓	✓	
Backup, doppelte Replikation und Doppelarchiv		✓	

Aufgabenkritische Modelle entwickeln sich zu einer Topologie für die wertvollsten Daten eines Unternehmens. Diese Daten sind für den Betrieb der Minimum Viable Company (MVC) erforderlich.

Was ist Ihr Minimum Viable Company?

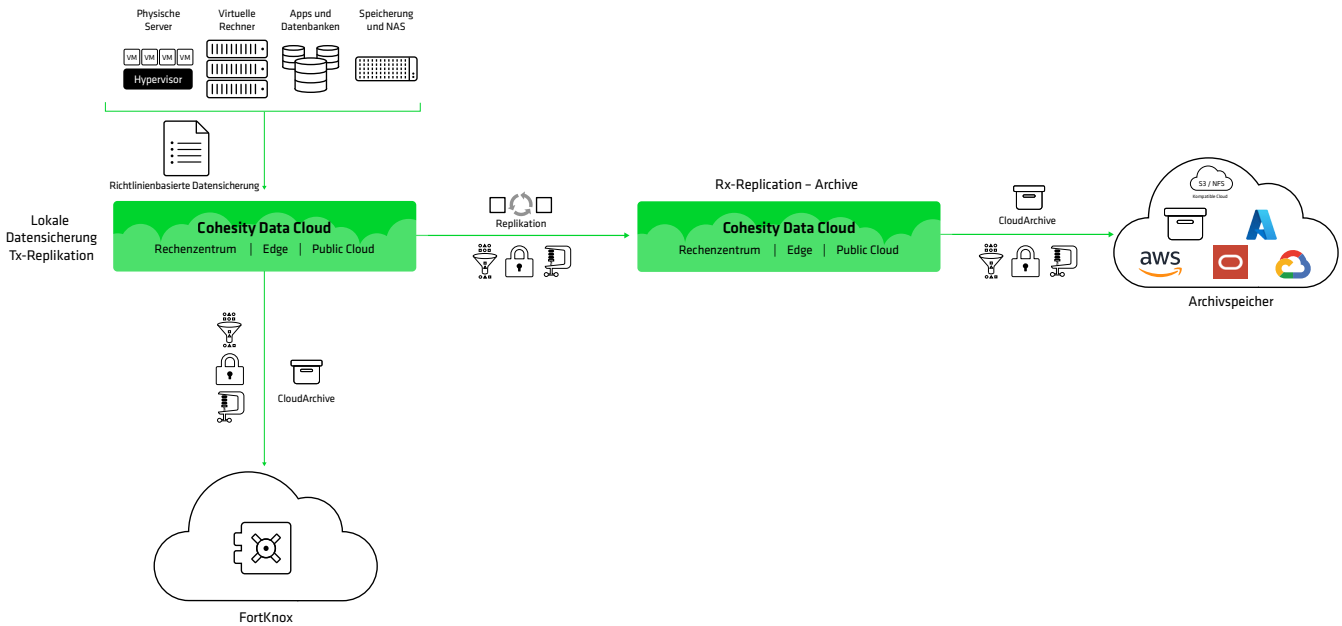
Ein MVC ist die Sammlung von Anwendungen, Infrastrukturen und Prozessen, die wiederhergestellt werden müssen, damit ein Unternehmen auf einem minimal lebensfähigen Niveau funktionieren kann. Diese Systeme müssen zuerst wieder online gebracht werden; alle anderen Systeme haben zweitrangige Priorität. IT-Führungskräfte müssen MVC bei der Planung ihrer Strategien zur Reaktion auf Vorfälle und zur Wiederherstellung sowie ihrer Datentopologie berücksichtigen.

Aufgabenkritisch: M1 – Backup und doppelte Replikation mit Archiv



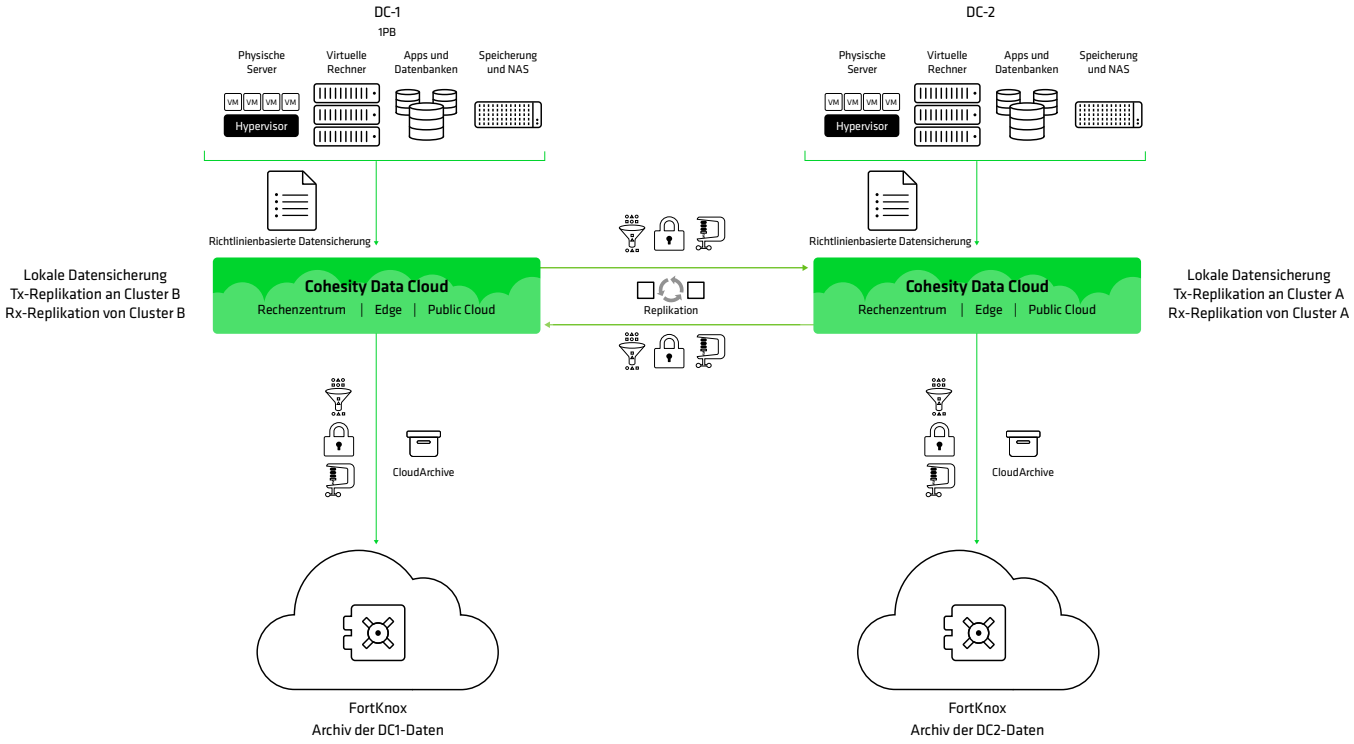
Diese fehlertolerante Architektur erfüllt strenge RTO- und RPO-Anforderungen und ist mit einer langfristigen Aufbewahrungspflicht verbunden. Das zweite Replikat bietet zusätzliche Notfallwiederherstellung und Schutz vor Ransomware. Mit der Cohesity Data Cloud kann ein Archiv über einen primären oder sekundären Cluster wiederhergestellt werden. Das Hinzufügen eines Air Gap zum zweiten Replikat sorgt für zusätzliche Ausfallsicherheit.

Aufgabenkritisch: M2 – Backup und Replikation mit Doppelarchiv unter Verwendung von FortKnox (aus lokalem Backup)



Diese fehlertolerante Architektur verwendet FortKnox anstelle eines zweiten Replikats, da FortKnox zusätzliche Sicherheit und Isolation bietet. Das erste Archiv kann für Compliance-Aktivitäten verwendet werden, während das FortKnox-Archiv für zusätzlichen Schutz vor Ransomware sorgt. Mit der Cohesity Data Cloud kann ein Archiv über einen primären oder sekundären Cluster wiederhergestellt werden.

Aufgabenkritisch: M2 – Cross-Replikation und Archiv von lokalem Backup mit FortKnox



Dies ist das **Active-Active**-Modell, das wir in den **Basic**-Topologien gesehen haben, ergänzt um duale FortKnox-Archive. Da jeder Cluster sowohl DC1- als auch DC2-Kopien enthält, enthält jede FortKnox-Instanz auch DC1- und DC2-Kopien. Mit der Cohesity Data Cloud kann ein Archiv über einen primären oder sekundären Cluster wiederhergestellt werden.

Aufgabenkritisch: M3 – Hub-and-Spoke mit Active-Active-Hubs und FortKnox-Archiv

Dies ähnelt dem, was wir bei den **erweiterten** Typen gesehen haben, aber in diesem Fall ist jedes Replikat als Langzeitarchiv mit FortKnox verbunden. Da die Replikate Kopien sowohl der linken als auch der rechten Spoke enthalten, verfügt auch jedes FortKnox-Archiv über beide Kopiensätze. Mit der Cohesity Data Cloud kann ein Archiv über einen primären oder sekundären Cluster wiederhergestellt werden.

Fazit und nächste Schritte

Viele Unternehmensleitungen möchten den Schutz ihrer kritischen Daten verbessern. Wenn wir mit diesen Entscheidungsträgern neue Ansätze diskutieren, sind Blueprints entscheidend. Die in diesem Whitepaper vorgestellten Konzepte helfen Führungskräften zu verstehen, was Kollegen in ähnlichen Situationen mit ähnlichen Datensicherungsanforderungen getan haben.

„Mehr" ist nicht immer besser, wenn es um Datenkopien geht. Sowohl Cohesity als auch unsere Kunden wissen, dass zusätzliche Datenkopien Betriebs-, Lizenz- und häufig auch Hardwarekosten verursachen. In manchen Fällen empfehlen wir nicht das Hinzufügen einer weiteren Kopie, sondern die Verwendung verschiedener Kopietypen.

Wir raten häufig, Archive für Compliance-Aktivitäten des Unternehmens und zur Förderung der Cyber-Resilienz zu nutzen. Daher entscheiden sich unsere Kunden oft dafür, die gleiche Anzahl von Datenkopien beizubehalten, aber die Art der verwendeten Kopien zu ändern. Sie können beispielsweise ein lokales, unsicheres Archiv durch ein isoliertes Archiv wie FortKnox ersetzen und somit Kopien bereitstellen, die sowohl für Compliance-Zwecke als auch für die Ransomware-Resilienz verwendet werden können.

Blueprints sind leistungsstark, da sie es Ihnen ermöglichen, alle relevanten, bewährten Optionen zu prüfen und eine fundierte Entscheidung darüber zu treffen, welche dieser Optionen Sie in Ihrer Bereitstellung verwenden möchten.

Das folgende Diagramm bietet eine vereinfachte, aggregierte Ansicht des Nutzens der einzelnen Topologien im Hinblick auf Fehlerdomänen, höhere Gewalt und Cyberschutz.

Typ	**Basic**		**Erweitert**	**Aufgabenkritisch**	
Kopien	**1**	**2**	**3**	**4**	**5**
Topologie	**Nur Backup**	**Backup und Repository** (Replikation oder Archiv)	**Backup und doppeltes Repository** (Replikation und Archiv oder doppelte Replikation)	**Backup und doppelte Replikation und Archiv**	**Backup und doppelte Replikation und Doppelarchiv**
Schutz vor HW- und SW-Fehlerdomänen	★	★ ★	★ ★ ★	★ ★ ★ ★	★ ★ ★ ★
Schutz vor „höherer Gewalt"		★	★ ★ ★	★ ★ ★ ★	★ ★ ★ ★
Cyberschutz	★	★ ★	★ ★ ★	★ ★ ★ ★	★ ★ ★ ★

Der Weg zu moderner Datensicherheit und -verwaltung mag entmutigend erscheinen. Wir haben diese Informationen zusammengestellt, um Ihnen die Arbeit zu erleichtern und Ihnen dabei zu helfen, schneller bessere Geschäftsergebnisse zu erzielen und gleichzeitig Risiken und Kosten zu reduzieren.

Daher empfehlen wir Ihnen folgende Schritte:

1. Bestimmen Sie, welche Blueprints für Ihre Situation am relevantesten sind.
2. Bewerten Sie den ROI und die Gesamtbetriebskosten einer modernen Datenplattform im Vergleich zu Ihrer bestehenden Lösung. Die wichtigsten Vergleichspunkte sollten sein:
    a. Effizienz der Datensicherung
    b. Betriebliche Effizienz
    c. Risiken und Compliance
3. Wählen Sie Ihre Lösung auf der Grundlage von Produktdemonstrationen, nachgewiesenen ROI- und TCO-Berechnungen und der Unterstützung der Roadmap-Prioritäten.
4. Implementieren Sie Ihre gewählte Lösung gemäß den relevantesten Blueprints und setzen Sie die Roadmap aus dem vorherigen Schritt um.

Sobald Ihre moderne Plattform eingerichtet ist, erstellen Sie erste KPIs zur Cyber-Resilienz und messen Sie Ihren Fortschritt regelmäßig anhand dieser Basiswerte. So wissen Sie, wann Sie mit der nächsten Phase Ihrer Reise fortfahren können.

Über Cohesity

Cohesity ist führend im Bereich KI-gestützte Datensicherheit. Mehr als 13.600 Unternehmenskunden, darunter über 85 der Fortune 100 und fast 70 % der Global 500, vertrauen auf Cohesity, um ihre Resilienz zu stärken und gleichzeitig Gen AI-Einblicke in ihre riesigen Datenbestände zu bekommen. Die Lösungen des Unternehmens, die aus dem Zusammenschluss von Cohesity und dem Datenschutzgeschäft von Veritas hervorgegangen sind, sichern und schützen Daten On-Premises, in der Cloud und am Edge Cohesity wird von NVIDIA, IBM, HPE, Cisco, AWS, Google Cloud und anderen unterstützt. Der Hauptsitz des Unternehmens befindet sich in Santa Clara, Kalifornien, mit Niederlassungen auf der ganzen Welt. Folgen Sie Cohesity auf **LinkedIn**, **X** und **Facebook**, um weitere Informationen zu erhalten.

Erfahren Sie mehr bei Cohesity

COHESITY

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

2000050-002 DE 4-2025