

Multicloud- Datenschutz und -Wiederherstellung

Lawrence Miller

- ✓ Herausforderungen des modernen Datenmanagements
- ✓ Anwendungsfälle für Multicloud-Datenschutz und -Wiederherstellung
- ✓ Anforderungen an eine Multicloud-Datenschutz- und -Wiederherstellungslösung

INHALT

Daten sind für moderne Unternehmen unverzichtbar, und ihr Verlust aufgrund von Ransomware, Hardwareausfällen oder anderen Problemen kann zu Betriebsausfällen führen. Um diese Risiken zu minimieren, sind eine effektive Datensicherung und -wiederherstellung unerlässlich. In diesem Tech-Brief werden die Herausforderungen und Lösungen im Bereich Datenmanagement, insbesondere in Multicloud-Umgebungen, beleuchtet.

Zu den Highlights gehören:

- Die Vorteile von Multicloud-Architekturen stehen im Widerspruch zu den Herausforderungen hinsichtlich Datenmanagement und -schutz.
- Zu den wesentlichen Funktionen für einen modernen Datenschutz gehören Cloud-native Unterstützung, sofortige Wiederherstellung und Cyber-Resilienz.

CONTENTS

- 2** Modern Data Management Challenges
- 4** Multicloud Data Protection and Recovery Use Cases
- 5** Requirements for a Multicloud Data Protection and Recovery Solution
- 6** Customer Story

Daten sind das Lebenselixier jedes modernen Unternehmens. Doch was passiert, wenn Ihre Daten verloren gehen? Ob durch Ransomware, einen Denial-of-Service-Angriff (DoS), einen böswilligen Insider, eine Hardware-Fehlfunktion oder einen Fehler – wenn Ihre Daten verloren gehen, kann Ihr Unternehmen nicht mehr arbeiten. Angesichts der kritischen Bedeutung von Daten für Unternehmen heutzutage müssen Sie sicherstellen, dass Sie Ihre Daten schnell und effektiv sichern und wiederherstellen können.

In diesem Tech-Brief erfahren Sie mehr über die Herausforderungen des Datenmanagements, Anwendungsfälle für den Schutz und die Wiederherstellung von Daten in mehreren Clouds sowie die Funktionen und Merkmale, die Sie in einer modernen Lösung für den Schutz und die Wiederherstellung von Daten benötigen.

Herausforderungen des modernen Datenmanagements

Obwohl sie wissen, wie wichtig der Schutz ihrer Daten ist, fällt es Unternehmen aufgrund komplexer IT-Infrastrukturen, Datensilos und eines explosionsartigen Datenwachstums schwer, diesen Schutz auch umzusetzen. Dies ist zum Teil darauf zurückzuführen, dass Unternehmen ein ganzes Sammelsurium an Datenschutz-Tools und -Produkten verwenden, um unterschiedliche Anwendungsfälle

Obwohl sie wissen, wie wichtig der Schutz ihrer Daten ist, fällt es Unternehmen aufgrund komplexer IT-Infrastrukturen, Datensilos und eines explosionsartigen Datenwachstums schwer, diesen Schutz auch umzusetzen.

abzudecken. Ein weiterer Grund sind klassische Lösungen, deren Wartung immer teurer wird und die nicht immer mit neuen Technologien kompatibel sind. Stattdessen setzen viele Firmen auf Cloud-First-Strategien mit Multicloud-Infrastrukturen.

In einer Multicloud-Architektur nutzt ein Unternehmen zwei oder mehr Cloud-Computing-Dienste von verschiedenen Cloud-Anbietern, mit dem Ziel, im Notfall Daten besser wiederherstellen zu können, Spitzentechnologien zu nutzen, Anwendungs-Workloads zu optimieren und Risiken zu minimieren. Das hat jedoch auch seine Nachteile – 87 % der Unternehmen, die eine Multicloud-Strategie verfolgen, geben an, dass die Verwaltung von Multicloud zu einer der drei größten Cloud-Herausforderungen für Unternehmen geworden ist.

Warum? Manchmal sind Multicloud-Architekturen eher unbeabsichtigt als Ergebnis eines dezentralen IT-Managements und einer flächendeckenden Schatten-IT entstanden und nicht als bewusste Strategie. Beispielsweise kann es sein, dass Ihre Personalabteilung eine Software-as-a-Service-Anwendung (SaaS) für die Gehaltsabrechnung verwendet, Ihre DevOps-Teams es vorziehen, Anwendungen auf Amazon Web Services (AWS) zu erstellen, und Ihre IT-Abteilung Ihre Kerninfrastruktur in Microsoft Azure verwaltet. Doch auch wenn sie bewusst gewählt werden, führen Multicloud-Strategien naturgemäß dazu, dass Daten an verschiedenen Orten gespeichert werden. Unabhängig davon, ob sie beabsichtigt waren oder nicht, sind Daten überall. Dies erhöht die Komplexität der IT und führt zu Herausforderungen beim Datenschutz und der Sicherheit.

Eine weitere Ursache für Datenwachstum und -komplexität ist die Datendemokratisierung, d. h. die Bereitstellung aller Daten und Datentypen für alle Benutzer im Unternehmen, anstatt das Sicherheitsprinzip der geringsten Privilegien anzuwenden, was zu weiteren Herausforderungen bei der Datenverwaltung führt. Da Unternehmen zunehmend eigene Initiativen im Bereich der künstlichen Intelligenz (KI) starten, werden die Datenmengen weiterhin exponentiell wachsen, und die Speicherung von Daten in unterschiedlichen Einzelprodukten, die in Multicloud- und Hybridarchitekturen eingesetzt werden, wird weiterhin immer problematischer.

Was Unternehmen brauchen, ist eine moderne Datenschutz- und Wiederherstellungslösung, die Systeme und Workloads in lokalen und hybriden Multicloud-Umgebungen schützt, vollständig integriert ist, granulare Sicherungs- und sofortige Wiederherstellungsfunktionen bietet, die Cyber-Resilienz stärkt, Bedrohungen erkennt und eine schnelle Wiederherstellung nach Cyberangriffen ermöglicht. Kurz gesagt: eine zentrale, einheitliche Lösung für Datenmanagement und -schutz, die heutige und zukünftige betriebliche Anwendungsfälle abdeckt.

Unternehmen benötigen eine moderne Lösung für Datenschutz und Wiederherstellung, die Cloud-nativ und vollständig integriert ist, granulare Backup- und sofortige Wiederherstellungsfunktionen bietet, die Cyber-Resilienz stärkt, Bedrohungen erkennt und eine schnelle Wiederherstellung nach Cyberangriffen ermöglicht.

Anwendungsfälle für Multicloud-Datenschutz und -Wiederherstellung

Multicloud-Datenschutz und -Wiederherstellung sind in vielen Anwendungsfällen sinnvoll. Zu den gängigsten gehören:

- **Sicherung und Wiederherstellung.** Daten können auf verschiedene Weise verloren gehen, böswillig oder nicht, weshalb ein kritischer erster Schritt zur Wiederherstellung die Sicherung Ihrer Daten ist. Es ist wichtig, über einen Prozess und ein Tool zu verfügen, um Kopien von Daten an einem sicheren Ort zu erstellen und zu speichern, sodass diese vor Verlust oder Beschädigung geschützt sind.
- **Datensicherheit und Compliance.** In verschiedenen Branchen gelten unterschiedliche Regeln für den Umgang mit Daten. So gilt beispielsweise die Datenschutz-Grundverordnung (DSGVO) für alle Unternehmen, die personenbezogene Daten von in der Europäischen Union ansässigen Personen kontrollieren oder verarbeiten. Unternehmen, die ihre Daten nicht gemäß den Vorschriften ihrer Branche verwalten, müssen mit rechtlichen, monetären und finanziellen Konsequenzen rechnen.
- **Schutz und Erkennung von Ransomware sowie Datenwiederherstellung.** Der wirksamste Schutz vor Ransomware ist ein gutes, unveränderliches Backup Ihrer Daten, das eine schnelle Wiederherstellung ermöglicht – ohne Lösegeld zu zahlen. Sie sollten jedoch auch eine Strategie für die richtige Reaktion auf eine Ransomware-Attacke entwickeln. Richten Sie Ihre Strategie an Richtlinien wie NIST aus, um sicherzustellen, dass Sie bewährte Verfahren für die Cybersicherheit anwenden und über robuste Schutz-, Erkennungs- und Wiederherstellungsfunktionen für Ihre Daten verfügen.
- **Langfristige Aufbewahrung und Archivierung.** Für Unternehmen, die regelmäßig neue Daten generieren, aber auch vorhandene Daten speichern müssen, ist die Datenarchivierung von entscheidender Bedeutung, da sie es Organisationen ermöglicht, beide Arten von Daten schnell abzurufen. In bestimmten Branchen ist die Aufbewahrung von Daten über längere Zeiträume aus Compliance- und regulatorischen Gründen erforderlich.
- **Notfallwiederherstellung und Betriebskontinuität.** In unserer schnelllebigen, „allzeit bereiten“ Geschäftswelt wirken sich Ausfallzeiten negativ auf Ihren Ruf und Ihr Geschäftsergebnis aus. Unternehmen müssen in der Lage sein, die immer strengeren Anforderungen an maximal tolerierbare Ausfallzeiten (MTD), Wiederherstellungszeitziele (RTO) und Wiederherstellungspunktziele (RPO) zu erfüllen, um sicherzustellen, dass ihr Geschäft nach einem Ausfall oder einem anderen schwerwiegenden Ereignis schnell und vollständig wiederaufgenommen werden kann.

Anforderungen an eine Multicloud-Datenschutz- und -Wiederherstellungslösung

Da Daten für Unternehmen immer wertvoller werden, ist eine moderne Datenschutz- und Wiederherstellungslösung für den Multicloud-Bereich unerlässlich. Zu den wichtigsten Anforderungen gehören:

- **Einheitliche Verwaltung.** Eine zentrale, einheitliche Lösung ermöglicht eine globale Verwaltung in Multicloud-, Hybrid- und lokalen Umgebungen in großem Maßstab. Sie sollte als intelligenter globaler Assistent fungieren, der potenzielle Ransomware-Angriffe erkennt, Ihnen bei der Identifizierung von Anomalien hilft und entsprechende Empfehlungen zur Fehlerbehebung gibt, z. B. für die Planung zusätzlicher Kapazitäten.
- **Schutz für lokale, Cloud- und SaaS-Daten.** Daten sind heute überall. Moderne Datenschutz- und Wiederherstellungsmaßnahmen müssen Ihre Daten unabhängig von ihrem Speicherort schützen, ob lokal, in Multicloud- und Hybridumgebungen oder in SaaS-Anwendungen. Achten Sie auf flexible lokale und Cloud-Bereitstellungsoptionen, die selbstverwaltet oder „as-a-Service“ verwaltet werden können.
- **Sofortige Massendatenwiederherstellung.** Angreifer versuchen, so viele unserer Daten wie möglich herauszufiltern oder zu zerstören, daher benötigen Sie eine Möglichkeit, alle Ihre Daten schnell wiederherzustellen. Suchen Sie nach einer Lösung, die Snapshots vollständig aktualisiert, um die Wiederherstellungszeiten zu verkürzen, sodass Hunderte von VMs, große Datenbanken und große Mengen unstrukturierter Daten sofort, in großem Umfang, zu jedem Zeitpunkt und an jedem Ort wiederhergestellt werden können.
- **Cyber-Wiederherstellung.** Überprüfen Sie die Vollständigkeit Ihrer Backups, um einen „sauberen“ Wiederherstellungspunkt zu ermitteln, z. B. im Falle eines Ransomware-Angriffs, der auf Backups abzielt. Suchen Sie nach einer Lösung, mit der Sie Daten auf granularer Ebene zuverlässig wiederherstellen können.
- **Unbegrenzte Skalierbarkeit.** Vermeiden Sie komplexe, riskante und kostspielige lokale Forklift-Upgrades und skalieren Sie Ihre Lösung einfach und unterbrechungsfrei. Suchen Sie nach einer Scale-out- und Hyperscale-Architektur und einem verteilten Dateisystem, das globale Suchfunktionen bietet und Ihnen dabei hilft, Ihren Daten- und Speicherplatzbedarf durch globale Deduplizierung und Komprimierung mit variabler Länge zu reduzieren.

Da Daten für Unternehmen immer wertvoller werden, ist eine moderne Datenschutz- und Wiederherstellungslösung für den Multicloud-Bereich unerlässlich.

Kundenbericht

Ausenco optimiert Sicherheit und Verwaltungsaufwand mit Cohesity DataProtect as a Service

Als multinationaler Anbieter von Ingenieurs- und Beratungsdienstleistungen sichert Ausenco 100 TB kritischer Microsoft 365 (M365)-Daten für seine mehr als 3.000 Mitarbeiter. Die vorherige Backup-Lösung - Veeam-Software auf einer selbst verwalteten Cloud-Infrastruktur - entsprach nicht mehr den Sicherheitsanforderungen des Unternehmens und kostete 20 Stunden pro Woche an Verwaltungsaufwand. Durch den Wechsel zu Cohesity DataProtect, das als Service bereitgestellt wird, sparte Ausenco 20 Stunden pro Woche, die zuvor für die Verwaltung der Backup-Infrastruktur aufgewendet wurden, führte 4-Stunden-Service-Level-Agreements (SLAs) für die Wiederherstellung von Dateien ein und bekam die unveränderlichen Backups, die für die Cyber-Versicherung und ein sorgenfreies Arbeiten erforderlich sind. Und das alles ohne zusätzliche Kosten.

HERAUSFORDERUNG

Ausencos Ingenieurs- und Beratungsgeschäft wächst - insbesondere bei Bergbauunternehmen, die eine steigende Nachfrage nach Batteriemetallen verzeichnen. Das Unternehmen sichert 100 TB an kritischen M365-Daten für seine mehr als 3.000 Mitarbeiter. „Microsoft bietet einen gewissen eingebauten Datenschutz, der aber für unser Geschäft nicht ausreicht“, sagt Kalpesh Bhathella, Director of Operational Services bei Ausenco. „Wir bewahren einige SharePoint- und OneDrive-Dateien auf unbestimmte Zeit auf und können es uns nicht leisten, sie durch Cyberangriffe zu verlieren.“

Bis 2022 sicherte das IT-Team von Ausenco die M365-Daten mit Veeam-Software und nutzte dafür Infrastruktur als Service (IaaS) von Amazon Web Services (AWS). Die Verwaltung der Infrastruktur und der Software war jedoch sehr aufwändig und nahm 50 % der Zeit eines IT-Administrators in Anspruch. Ein weiteres Manko: Die Erstellung

unveränderlicher Sicherungskopien, ein Muss für die Wiederherstellung nach Cyberangriffen, würde mehr Infrastruktur und mehr Verwaltungszeit erfordern. „Sicherheit steht für uns an erster Stelle“, sagt Bhathella. „Potenzielle Kunden fragen immer danach, und neuerdings wollen sie auch wissen, ob wir eine Cyber-Versicherung haben. Wir brauchten unveränderbare Kopien, aber ohne zusätzlichen Verwaltungsaufwand.“

LÖSUNG

Nach Prüfung von Cohesity und Rubrik entschied sich Ausenco für Cohesity DataProtect, das als Service bereitgestellt wird und Backup- und Wiederherstellungsfunktionen für Software-as-a-Service (SaaS) wie M365 sowie für andere Cloud- oder On-Premise-Daten bietet, die Ausenco später hinzufügen könnte. „Uns gefiel die Idee eines komplett verwalteten Cloud-Dienstes, denn eine selbstverwaltete Infrastruktur ist heutzutage nicht sinnvoll, wenn IT nicht Ihr Kerngeschäft ist“, so Bhathella. Und nur Cohesity erstellt standardmäßig unveränderliche Backups.“

Der Cohesity-Cloud-Service war bereits nach etwa zwei Wochen einsatzbereit. Das IT-Team muss sich kaum noch damit befassen. „Nach der Erstkonfiguration lief Cohesity einfach“, meint Bhathella. „In den seltenen Fällen, in denen wir Support brauchten, hat Cohesity das Problem sofort gelöst. Wir mussten nie eskalieren.“

ERGEBNIS

Für Ausenco liegt der größte Vorteil der Cohesity-Lösung in der höheren Sicherheit. „Wir tun alles, um Cyberangriffe zu verhindern, aber die Möglichkeit, saubere M365-Daten aus den unveränderlichen Sicherungskopien von Cohesity wiederherzustellen, bedeutet, dass wir einen soliden Plan B haben. Durch die externe Speicherung unveränderlicher Sicherungskopien konnten wir uns außerdem für eine Cyber-Versicherung qualifizieren, nach der potenzielle Kunden fragen.“

Mehr Sicherheit kostet weniger, nicht mehr. „Die Einsparungen durch den Wegfall der monatlichen Gebühren für die Cloud-Infrastruktur haben Cohesity DataProtect as a Service vollständig bezahlt gemacht“, so Bhathella. „Darüber hinaus sparen wir die 20 Stunden pro Woche, die wir früher für die Abstimmung und Verwaltung unserer Backup-Software und Cloud-Infrastruktur aufgewendet haben.“ Das Teammitglied, das früher 50 % seiner Zeit mit der Verwaltung von Backups beschäftigt war, kann diese Zeit nun für höherwertige Aufgaben im Bereich der digitalen Transformation nutzen. Und zusammen mit den anderen Cybersicherheitsmaßnahmen von Ausenco haben unveränderliche Backups dem Unternehmen geholfen, sich für günstige Tarife bei seiner Cyber-Versicherung zu qualifizieren.

Zum ersten Mal bietet Ausenco eine 4-Stunden-SLAs für die E-Mail- oder Dateiwiederherstellung von M365 an – ein großer Erfolg bei den vielbeschäftigten Ingenieurs-, Beratungs- und operativen Teams des Unternehmens. „Mit unserer alten Backup-Lösung konnte die Wiederherstellung einer verlorenen Exchange-, SharePoint- oder OneDrive-Datei Wochen dauern, weil unser IT-Administrator Hunderte von Backups durchkämmen musste, um sie zu finden“, sagt Bhathella. „Die Suchmaschine von Cohesity ist wie ein Google für Backups. Wir geben einfach einen Dateinamen oder Satz ein, und schon wird eine Liste angezeigt. Die gesuchte Datei steht oft ganz oben.“

Derzeit bereitet sich Ausenco darauf vor, mit Cohesity DataProtect as a Service neben M365 auch andere Workloads zu schützen, wie lokale und virtuelle AWS-Maschinen. Für zusätzliche Ausfallsicherheit plant Bhathella, bestimmte Workloads auf Microsoft Azure zu sichern – eine Hybrid-Cloud-Einrichtung. Das IT-Team kann Backups und Wiederherstellungen in jeder Cloud über dieselbe Cohesity-Oberfläche anzeigen und verwalten und so die Vorteile einer einheitlichen Verwaltung nutzen.

Bhathella fasst zusammen: „Mit Cohesity DataProtect as a Service haben wir alles, was wir brauchen, um jede Art von Daten zu schützen, während unser Unternehmen wächst: unveränderliche Backups, schnelle Wiederherstellungen und hervorragenden Support – und das alles, ohne uns um das Infrastrukturmanagement kümmern zu müssen.“

Zu den wesentlichen Vorteilen der Cohesity-Lösungen gehören:

- **Unveränderliche Kopien – eine Voraussetzung für Cyber-Versicherungen**
- **Bis zu 99 % schnellere Wiederherstellung von M365-E-Mails und -Dateien – 4 Stunden statt 2 Wochen**
- **20 Stunden weniger Verwaltungsaufwand pro Woche**
- **Keine zusätzlichen Kosten**

MEHR ZUM THEMA

Besuchen Sie <https://www.cohesity.com/de-de/solutions/backup-and-recovery> tum mehr über moderne Lösungen für Datenschutz und-wiederherstellung zu erfahren.

COHESITY