Clumio

eBOOK

Der ultimative Leitfaden zur Überwindung von Herausforderungen in AWS

Commvault®

Contents

01

Den vollen Wert der Cloud erkennen und nutzen

In den vergangenen Jahren haben zahlreiche Unternehmen ihre digitale Transformationsreise angetreten, um ihre Services zu modernisieren und die Kundenerfahrung zu verbessern. Das Jahr 2020 stellte Unternehmen jeder Größe vor zusätzliche Herausforderungen und zwang sie, ihre Betriebsmodelle grundlegend zu überdenken. Digitale Transformation ist nicht länger nur eine Option, um wettbewerbsfähig zu bleiben – sie ist zu einer zwingenden Voraussetzung für den Erfolg geworden. An einen physischen Standort gebunden zu sein, um tägliche Geschäftsabläufe sicherzustellen, ist in der heutigen Welt keine Option mehr. Stattdessen ist es essenziell, in der Lage zu sein, den Betrieb von jedem beliebigen Ort aus effizient zu gewährleisten.

Öffentliche Clouds wie AWS bieten seit Langem die Möglichkeit, dieses Ziel zu erreichen – und im Jahr 2020 nahm die Geschwindigkeit der Cloud-Migration deutlich zu. Die treibenden Kräfte hinter der Verlagerung in die Cloud beinhalten den Zugang zu modernster Technologie, die Fähigkeit, schneller zu innovieren, sowie die Entlastung von der Verwaltung eigener IT-Infrastruktur. Diese Vorteile ermöglichen es Unternehmen, sich stärker auf ihr Kerngeschäft zu konzentrieren und deutlich schneller zu wachsen.

Die Cloud ist gekommen, um zu bleiben, und nahezu jedes Unternehmen wird künftig eine Cloud-Präsenz besitzen. Mit dem rasanten Innovationstempo seines Serviceangebots ist AWS für viele Organisationen die bevorzugte Cloud-Plattform. Doch trotz aller Vorteile von AWS gibt es auch erhebliche Herausforderungen, die verhindern können, das volle Potenzial der Cloud auszuschöpfen.

Schutz von Daten in AWS

Der Schutz von Unternehmens- und Kundendaten in der Cloud stellt eine der zentralen Herausforderungen dar. Eine solide Backup- und Recovery-Strategie in AWS ist genauso wichtig wie in der On-Premises-Welt – wenn nicht sogar wichtiger. In vielerlei Hinsicht ist sie zudem anspruchsvoller.

Durch die höhere Innovationsgeschwindigkeit in der Cloud können Unternehmen ihre Anwendungen deutlich schneller bereitstellen und skalieren. Dadurch entstehen enorme Mengen an produktiven Daten, die geschützt werden müssen. Gleichzeitig sind die Daten in der Cloud stärker verteilt – über verschiedene Anwendungen, Konten, Regionen und sogar unterschiedliche Public Clouds hinweg.

Auch die Angriffsfläche ist wesentlich größer, was zu einem deutlichen Anstieg von Angriffen führt. Schließlich befinden sich Unternehmen aus Sicht des Datenschutzes in einer deutlich dezentraleren Umgebung als in der traditionellen On-Premises-Welt.

Ist AWS Backup die Lösung?

Viele Unternehmen beginnen ihre Cloud-Nutzung mit „Schatten-IT"-Projekten oder im Rahmen einer digitalen Transformationsinitiative, bei der die Cloud-Migration ein zentraler Bestandteil der Strategie ist. AWS macht es Ingenieuren leicht, einige EC2-Instanzen bereitzustellen und erste Datenbank-Workloads in RDS auszuführen.

Sobald diese Initiativen jedoch Fahrt aufnehmen, wird schnell klar, dass für all diese neuen Cloud-Workloads keine solide Datenschutzstrategie existiert – kein durchdachter Backup- und Recovery-Plan. Schließlich gehört Backup nicht zum üblichen Vokabular eines Ingenieurs, und viele gehen davon aus, dass AWS sich bereits um alles kümmert. Doch beim Thema Datenschutz ist es oft schwierig zu wissen, wo man in der Cloud beginnen soll.

Ein naheliegender Weg besteht darin, die nativen Backup-Services von AWS zu nutzen. Eine der gängigsten Methoden, wie Unternehmen den Datenschutz in AWS umsetzen, ist der Einsatz des Snapshot-Management-Services.

Auf den ersten Blick erscheinen Snapshots mit 0,05 USD/GB pro Monat relativ kostengünstig. Unternehmen gehen davon aus, dass sie über die AWS Management Console mühelos Snapshots erstellen können. Um auf Nummer sicher zu gehen, handeln manche Organisationen sogar vorschnell und erstellen mit wenigen Mausklicks Snapshots aller EBS- und RDS-Volumes – einfach, um kein Risiko einzugehen.

Der Eindruck entsteht, dass der Datenschutz unter Kontrolle ist. Aber der Schein trügt.

02

Die Herausforderungen von AWS Backup

Leider dauert es nicht lange, bis Unternehmen die Grenzen von Snapshots erkennen, wenn es darum geht, geschäftskritische Unternehmens- und Kundendaten auf AWS zu schützen. Während Snapshots grundlegende Datenschutzfunktionen bieten – etwa die Wiederherstellung nach Bedienfehlern –, reichen sie bei weitem nicht aus, um eine umfassende, gleichzeitig einfache und kosteneffiziente Datenschutzlösung bereitzustellen.

Tatsächlich sind Snapshots bestenfalls rudimentär und erfordern komplexe, zeitaufwendige Prozesse, um selbst alltägliche Aufgaben auszuführen – was dem eigentlichen Zweck der Nutzung einer Public Cloud widerspricht.

Letztlich garantieren Cloud-Anbieter, einschließlich AWS, die Sicherheit der Infrastruktur – jedoch nicht die Sicherheit der darauf befindlichen Daten. Die Verantwortung für das Datenmanagement liegt weiterhin beim Kunden.

Um den vollen Nutzen von AWS ausschöpfen zu können, ist es daher entscheidend, dass Unternehmen den Datenschutz in der Cloud richtig umsetzen.

Werfen wir nun einen genaueren Blick darauf, warum die Nutzung von Snapshots für Backup und Recovery in AWS so problematisch ist.

Kein Air Gap

Ransomware-Angriffe steigen rasant an, und die Angst davor, dass Kriminelle Unternehmensdaten als Geiseln halten, entwickelt sich zunehmend zum schlimmsten Albtraum vieler CIOs und IT-Entscheidungsträger. Laut Cybersecurity Ventures werden die Schäden durch Ransomware bis 2031 voraussichtlich jährlich rund 275 Milliarden US-Dollar betragen – bei einem neuen Angriff alle 2 Sekunden.

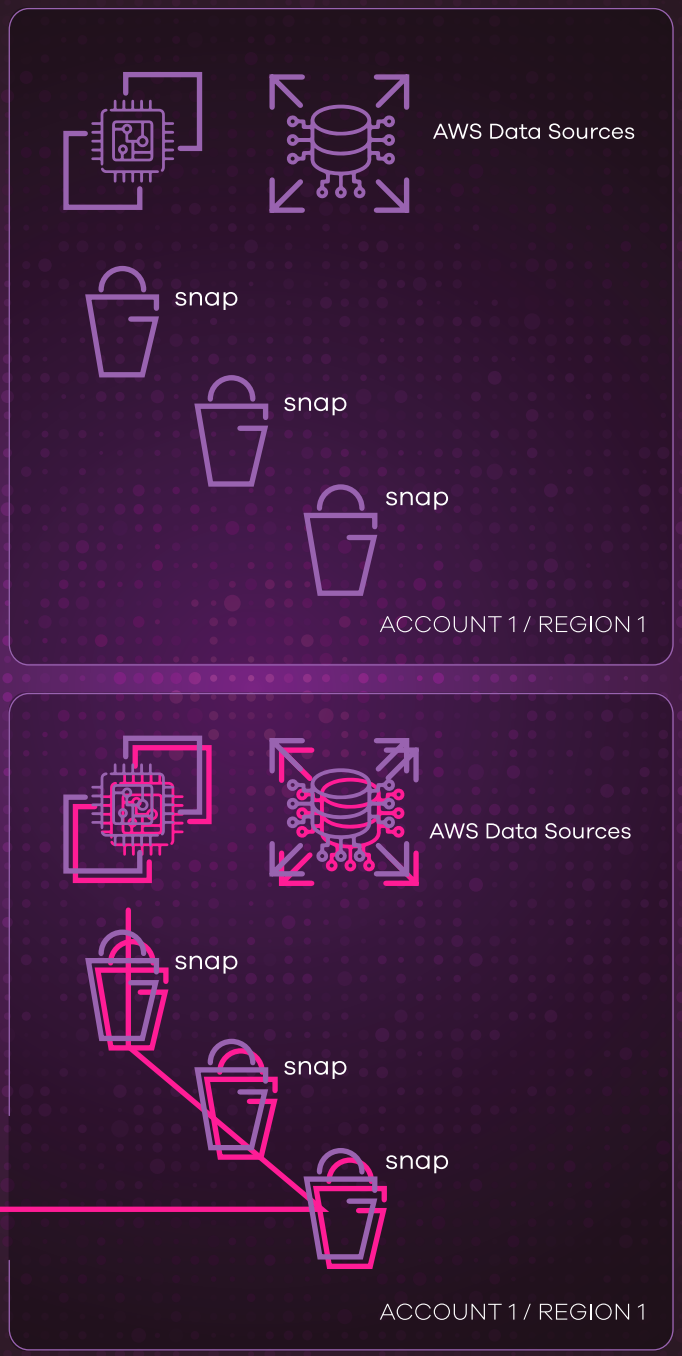
Daher ist es von entscheidender Bedeutung, über eine wirksame Cyber-Resilienz-Lösung zu verfügen, die hilft, solche Angriffe abzuwehren. Experten wie die CISA (Cybersecurity and Infrastructure Security Agency) empfehlen hierfür eine Lösung mit air-gapped Backup-Daten – also Datensicherungen, die unabhängig geschützt, separat gespeichert und vollständig vom Sicherheitsbereich der Organisation isoliert sind. Dadurch wird verhindert, dass Angreifer die Backup-Kopien entdecken, selbst wenn sie bereits Zugriff auf das Cloud-Konto erlangt haben.

Wie dargestellt, werden bei der Nutzung von AWS Backup zum Schutz von Datenquellen wie EC2, EBS oder RDS die Snapshots im selben Konto erstellt wie die primären Datenquellen. Das Problem an diesem Ansatz ist, dass es keine Trennung oder keinen Air Gap zwischen den primären Daten und den Snapshots gibt.

Zwar hat AWS für einige Ressourcen logisch isolierte („air-gapped“) Vaults eingeführt, jedoch befinden auch diese sich weiterhin innerhalb der Sicherheitsumgebung des Unternehmens und könnten somit ebenfalls kompromittiert werden.

Gelangt ein Hacker oder ein böswilliger Akteur in das primäre Konto, wird er zuerst die Snapshots kompromittieren und anschließend die primären Daten. In diesem Moment existiert keine gültige oder nutzbare Sicherungskopie mehr – und damit auch keine Möglichkeit, die ursprünglichen Daten wiederherzustellen.

Genau in dieser Situation möchten Unternehmen sich nicht wiederfinden. Und genau deshalb stellt dieser Aspekt eine erhebliche Einschränkung der Datenschutzmechanismen in der Cloud dar.



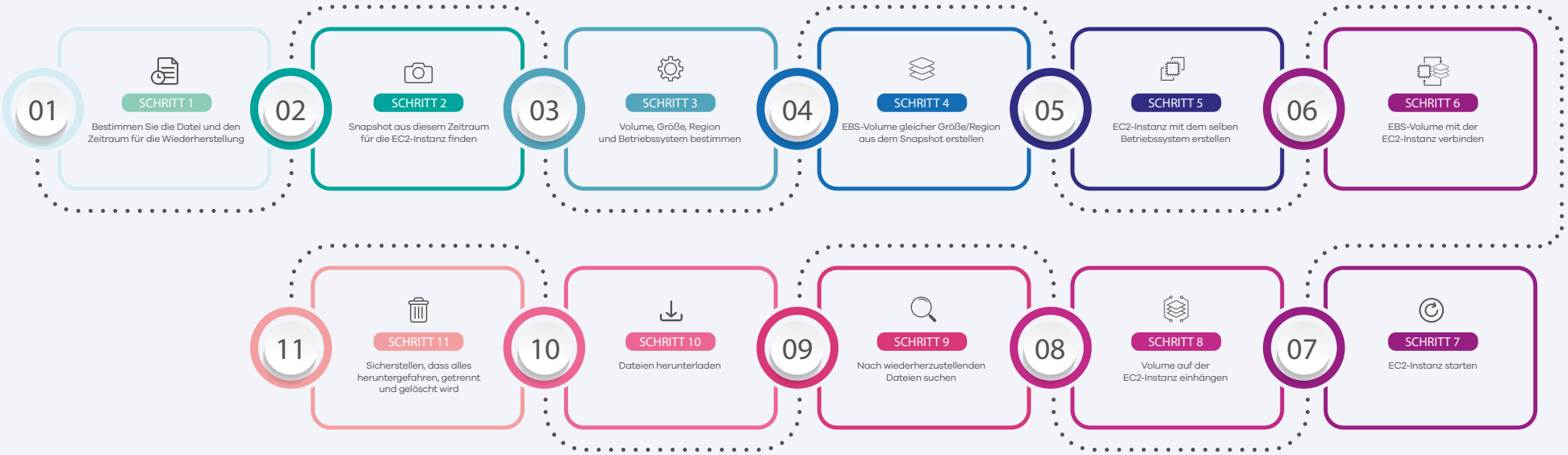
Lange Wiederherstellungszeiten

Datenschutz umfasst zwei grundlegende Funktionen: Backup und Wiederherstellung. Während es wichtig ist, sicherzustellen, dass alle geschäftskritischen Daten zuverlässig gesichert werden, ist es ebenso wichtig, über eine Lösung zu verfügen, die im Falle eines Datenverlusts oder einer Kompromittierung eine schnelle Wiederherstellung ermöglicht. Wenn Unternehmen ihre Daten nicht rechtzeitig wiederherstellen können, führt dies zu Unterbrechungen der Geschäftskontinuität, zu einer schlechten Kundenerfahrung und kann im Extremfall sogar das Fortbestehen einer Organisation gefährden.

Bei der Wiederherstellung geht es nicht nur darum, Zugriff auf Daten zu erhalten, sondern auch darum, wie lange es dauert, diese Daten in einer feingranularen Form wieder verfügbar zu machen. Die Wiederherstellung von Daten aus über AWS erstellten Snapshots kann mehrere Stunden, wenn nicht sogar Tage, in Anspruch nehmen.

Der Wiederherstellungsprozess lässt sich mit zahlreichen Kisten voller Akten in einem Lager vergleichen. Bei Snapshots gibt es nahezu keine Transparenz darüber, was in jeder einzelnen Kiste enthalten ist. Unternehmen müssen die Kisten öffnen und jede Datei einzeln durchsuchen. Sie müssen sich mühsam durch die Kisten arbeiten, um herauszufinden, welche Datei die richtige ist. Wenn sie glauben, die benötigte Datei gefunden zu haben, starten sie den Wiederherstellungsvorgang – und müssen anschließend warten, bis der gesamte Prozess abgeschlossen ist. Schon dieser Schritt allein kann erheblich viel Zeit kosten.

Bei der Wiederherstellung geht es nicht nur darum, Zugriff auf Daten zu erhalten, sondern darum, wie lange es dauert, diese Daten in granularer Form wieder bereitzustellen.



Dann muss das wiederhergestellte Volume auf einem Server eingehängt werden. Anschließend muss es geladen und überprüft werden, um festzustellen, ob es tatsächlich die gewünschten Daten enthält. Häufig stellt sich dabei heraus, dass die benötigte Datei nicht vorhanden ist oder nicht in der richtigen Version vorliegt – und dann beginnt die Suche in den „Boxen“ von vorne. Dieser gesamte Prozess kann leicht mehrere Stunden dauern.

Schauen wir uns ein typisches Szenario an, um diesen Punkt zu verdeutlichen. Eine Organisation verwendet AWS Backup zum Schutz ihrer EBS-Volumes und muss nun eine bestimmte Datei aus einem kompromittierten Volume wiederherstellen. Um diese Datei wiederherzustellen, müssen in AWS die folgenden komplizierten Schritte durchgeführt werden.

Je nachdem, wie lange es dauert, im zweiten Schritt den richtigen Snapshot zu finden, im dritten bis fünften Schritt das passende Betriebssystem, die richtige Volume-Größe, die Region usw. zu identifizieren und schließlich eine EC2-Instanz zu erstellen, die der ursprünglichen Instanz entspricht, kann der gesamte Vorgang mehrere Stunden in Anspruch nehmen. Und diese komplexen Arbeitsschritte müssen für jede einzelne Datei wiederholt werden, die wiederhergestellt werden soll.

Bei RDS ist die Situation sogar noch schlimmer, da zur Wiederherstellung einzelner Daten ein komplettes RDS-Instance-Restore erforderlich ist – selbst dann, wenn lediglich ein oder zwei Datensätze benötigt werden.

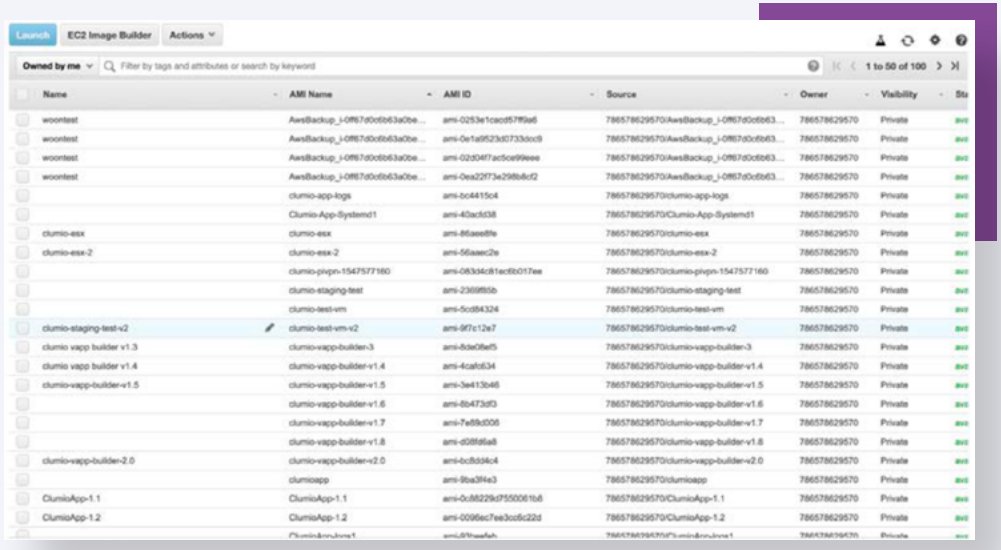
Abschließend müssen Unternehmen sicherstellen, dass alle Ressourcen, die in der Cloud zur Wiederherstellung der Datei bereitgestellt wurden, wieder gelöscht werden, um unnötige Kosten zu vermeiden.

Keine Transparenz

Das Festlegen von Datenschutzrichtlinien für alle Anwendungen ist keine tägliche Aufgabe. Tatsächlich sollten diese Richtlinien einmal richtig definiert und anschließend nur selten geändert werden, um Compliance-Anforderungen einzuhalten. Bei diesem Vorgehen ist es für IT-Administratoren nicht einfach, sich jede einzelne Richtlinie, jede Sicherungshistorie und jede Compliance-Vorgabe für jede geschützte Datenquelle im Umfeld zu merken.

Gleichzeitig ist es jedoch wichtig, diese Informationen bei Bedarf sofort griffbereit zu haben. Beispielsweise sollten Administratoren in der Lage sein:

- Während Audits schnell die Einhaltung von Richtlinien nachzuweisen
- Während des Wiederherstellungsprozesses problemlos den richtigen Snapshot zu finden
- Die passende Richtlinie auszuwählen, um eine neue Anwendung oder Datenquelle zu schützen
- All dies über Hunderte von Accounts hinweg durchzuführen



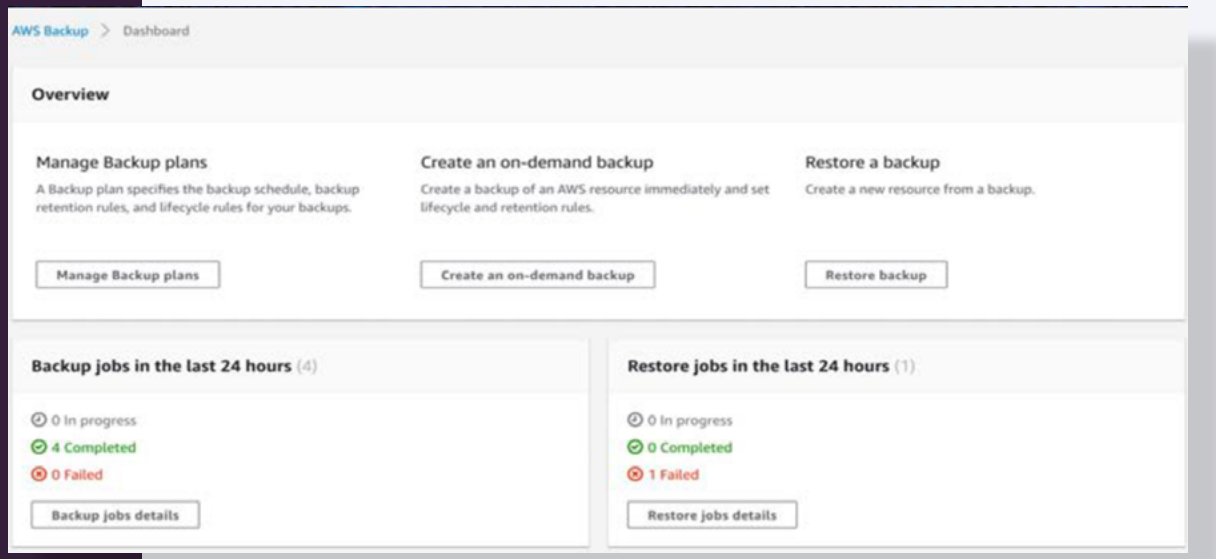
Viele Snapshots zum Durchscrollen

Es ist kompliziert und zeitaufwendig, den richtigen Snapshot für eine Wiederherstellung zu finden.

AWS Backup bietet die oben genannten Funktionen nicht, was zu einer eingeschränkten Sichtbarkeit Ihres gesamten Datenschutzkonzepts führt. Sehen wir uns ein praxisnahes Beispiel an, das die potenziellen Gefahren für ein Unternehmen verdeutlicht.

IT-Abteilungen werden häufig geprüft, um nachzuweisen, dass sie verschiedene Compliance-Standards erfüllen. Ein Versicherer könnte beispielsweise verlangen, dass ein Unternehmen nachweist, dass es über 30 Tage an Backups verfügt. Um dies mit AWS Backup nachzuweisen, müsste eine Organisation entweder Code schreiben, der dies belegt, oder die Anforderungen manuell für den Auditor zusammenstellen. Ein manueller Prozess birgt jedoch Fehlerquellen und zusätzliche Risiken sowohl für die Datensicherheit als auch für die Compliance.

Je nach Prüfplan muss die IT-Abteilung diesen mühsamen Prozess möglicherweise mehrmals im Jahr durchlaufen – oft verbringen Teams bis zu einer Woche damit, Berichte für Auditoren zu erstellen, zusätzlich zu ihren regulären Aufgaben.



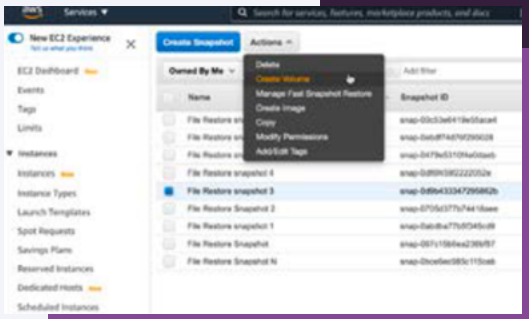
Keine Transparenz bei der Compliance

Zusätzliche Komplexität

Aus den bisher beschriebenen Lücken im AWS-Backup sollte deutlich geworden sein, dass Snapshots nur sehr grundlegende Funktionen bieten. Unternehmen, die Snapshots zur Sicherung ihrer AWS-Daten einsetzen, stoßen schnell auf diese Einschränkungen und sehen sich gezwungen, darauf zu reagieren.

Sie beginnen damit, komplexe Skripte zu schreiben, um fehlende Funktionen in ihre Datenschutzlösung zu integrieren. Dadurch müssen wertvolle IT-Ressourcen eingesetzt werden, um diese Skripte kontinuierlich zu entwickeln und zu pflegen – statt sich auf das Kerngeschäft zu konzentrieren.

Dies entspricht nicht dem eigentlichen Ziel der Cloud-Nutzung, nämlich die Agilität zu steigern und Innovationen schneller voranzutreiben.



Nur Wiederherstellung ganzer Instanzen

Eingeschränkte Instanz-Wiederherstellung nur im selben Konto

Nicht verfügbar	**Durchsuchen und Wiederherstellen**
Nicht verfügbar	**Globale Suche**
Nicht verfügbar	**Granulare Wiederherstellung einzelner Datensätze**

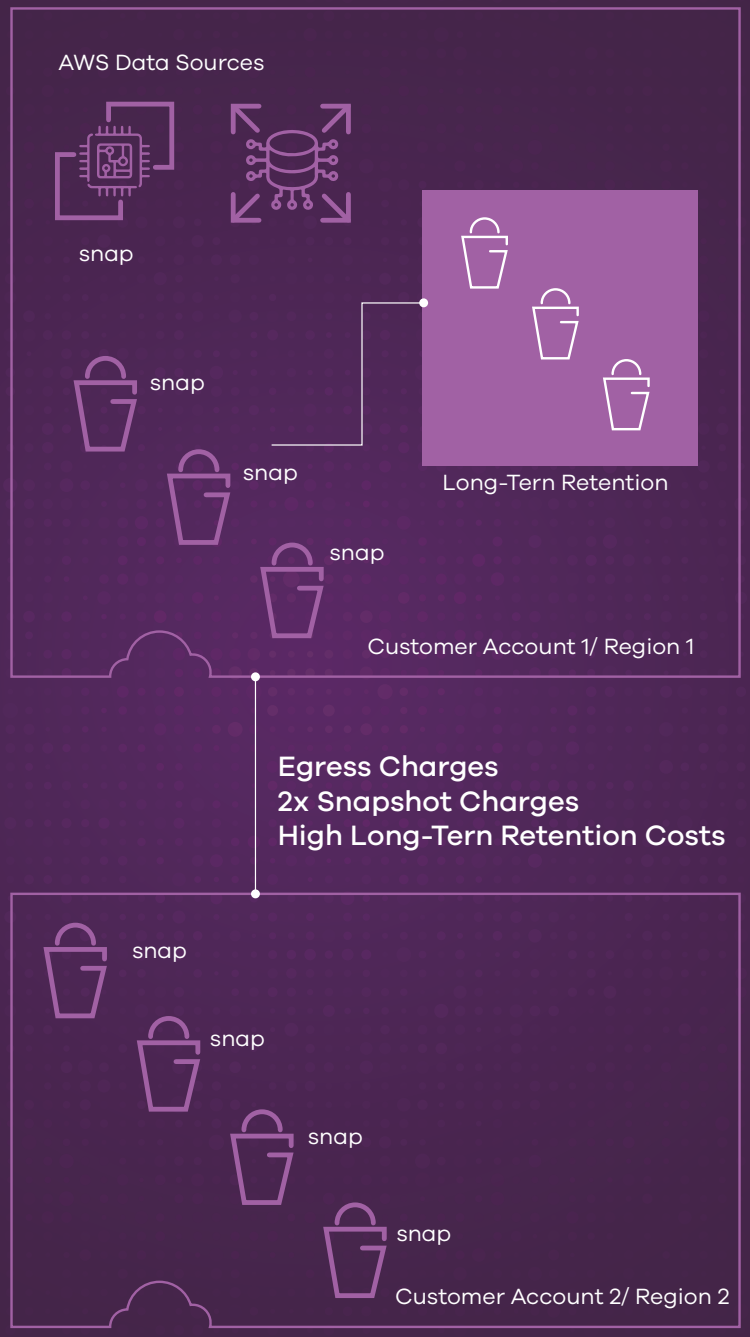
Schutz von Daten in AWS

Im Rahmen einer umfassenden Datenschutzstrategie ist es für Unternehmen üblich, eine langfristige Aufbewahrung von produktiven Daten einzurichten sowie Schutzmaßnahmen gegen Kontokompromittierungen, beispielsweise durch Ransomware-Angriffe. Um diese beiden Ziele mit AWS Backup zu erreichen, führen Organisationen in der Regel Folgendes durch:

- Erstellung von langfristigen, snapshotbasierten Aufbewahrungen, was zu einer großen Anzahl von Snapshots pro Account in hochpreisigen Speicherklassen führt
- Replikation von Snapshots von einem Konto in ein anderes, um sich vor Konto-kompromittierungen zu schützen – was die Anzahl der Snapshots verdoppelt und somit die Backup-Kosten ebenfalls erhöht. Zusätzlich fallen Egress-Gebühren für kontenübergreifende Transfers an

In einem typischen Szenario vergehen einige Monate, und ein Unternehmen beginnt, einen bedenklichen Trend zu erkennen. Die AWS-Rechnung steigt kontinuierlich an und zeigt keinerlei Anzeichen einer Stabilisierung. Gleichzeitig ist völlig unklar, was genau die steigenden AWS-Backup-Kosten verursacht.

Unterdessen kann der Datenschutz mit AWS das Unternehmen bis zu 50 Prozent mehr kosten.



Die Herausforderung durch Snapshot-Manager von Drittanbietern

Wenn Unternehmen beginnen, ihre AWS-Backup-Kosten besser zu verstehen und zu kontrollieren, wenden sie sich häufig Snapshot-Managern von Drittanbietern zu. Diese Anbieter werben damit, die Kosten deutlich senken zu können, indem sie beispielsweise ein Tiering zu S3 ermöglichen. Auf den ersten Blick wirkt die Preisgestaltung oft attraktiv – häufig als Lizenzgebühr pro Instanz dargestellt.

In der Realität sind die Gesamtkosten jedoch höher, da zusätzlich zu den Lizenzkosten weiterhin die AWS-Speicherkosten für die Daten anfallen sowie häufig auch die Kosten für die Compute-Ressourcen, die zur Ausführung des Backup-Managements erforderlich sind.

Beispielsweise zahlen Unternehmen für ein typisches EBS-Volume mit täglichen Änderungen weiterhin die AWS-Gebühr von 0,05 USD/GB/Monat für die zugrunde liegende Snapshot-Speicherung – und die Lizenzgebühr des Drittanbieters kommt oben drauf. Das führt unmittelbar zu einem Kostenaufschlag.

Darüber hinaus betreiben viele dieser Lösungen eigene EC2-Instanzen im Kundenkonto, etwa Backup-Manager-Instanzen und temporäre Worker-Instanzen, die zusätzliche, gemischte Nutzungskosten auf der AWS-Rechnung verursachen.

Die Kosten pro geschützter EC2-Instanz pro Monat mögen angemessen erscheinen, aber die tatsächlichen Gesamtkosten liegen deutlich höher.

Weitere versteckte Kosten

Doch sparen Unternehmen tatsächlich Geld durch die Tiering-zu-S3-Funktion? Um diese Funktion anbieten zu können, starten Snapshot-Manager von Drittanbietern temporäre EC2-Instanzen, die über längere Zeiträume laufen und Ihrer AWS-Rechnung versteckte Kosten hinzufügen. Diese Kosten sind nicht sofort ersichtlich, da sie sich mit Ihren regulären EC2-Ausgaben vermischen.

Die temporären EC2-Instanzen müssen die EBS-Snapshots eines Unternehmens durchlaufen und Datenblöcke nach S3 kopieren. Allein durch diese versteckten Kosten liegt der Break-even-Punkt fürs Verschieben nach S3 häufig bei etwa drei Monaten. Das bedeutet: Wenn ein Unternehmen tägliche Backups mit einer Aufbewahrungsfrist von weniger als drei Monaten hat, könnte es tatsächlich mehr ausgeben, als wenn es die Daten einfach in EBS-Snapshots belassen hätte.

Berücksichtigt man zusätzlich die zuvor erwähnten Lizenzkosten, steigen die Gesamtkosten noch weiter.

Und da EBS-Snapshots inkrementell sind, ist es für das S3-Tiering schwer, ausschließlich die wirklich benötigten Daten zu verschieben. Der Grund dafür ist, dass tägliche Snapshots (die nicht nach S3 verschoben werden sollten) möglicherweise auf ältere Datenblöcke verweisen, die Teil einer jährlichen Sicherung sind, die bereits nach S3 übertragen wurde.

Aufgrund dieser Komplexität ist es sehr wahrscheinlich, dass der Backup-Manager große Teile Ihrer Daten sowohl in EBS-Snapshots als auch in S3 gespeichert hat.

eBOOK

Benutzerdefinierte AWS-Backup-Skripte

Das Management erkennt schließlich, wie viel für AWS-Backups ausgegeben wird – insbesondere für den Drittanbieter-Manager. Dies führt dazu, dass ein gemeinsamer Engineering-Ressourcenpool bereitgestellt wird, um benutzerdefinierte Backup-Skripte zu entwickeln, die die Backup-Anforderungen des Unternehmens erfüllen können.

Nachdem die Organisation genügend Zeit und Aufwand investiert hat, läuft schließlich alles wie gewünscht: Die Skripte sind lizenzfrei, und das Unternehmen hat das Gefühl, seine Backup-Richtlinien nun im Griff zu haben. Doch sobald AWS seine APIs ändert oder sich geschäftliche Anforderungen weiterentwickeln – etwa das Bedürfnis, Backups regionsübergreifend zu erstellen oder sie vor Ransomware zu schützen –, müssen auch die Skripte angepasst werden.

Die ursprünglich geteilte Engineering-Ressource entwickelt sich zu einer Vollzeitstelle. Und nun hat das Unternehmen einen neuen, wenig versteckten Kostenfaktor: den Aufwand für die Verwaltung, Weiterentwicklung und Erstellung benutzerdefinierter Backup-Skripte.

Nun hat das Unternehmen einen nicht mehr ganz so versteckten Kostenfaktor für die Verwaltung, Verfeinerung und Erstellung benutzerdefinierter Backup-Skripte.

03

Commvaults Ansatz für den AWS-Datenschutz

Angesichts all der zuvor beschriebenen Herausforderungen – lange Wiederherstellungszeiten, fehlender Air Gap, mangelnde Transparenz, steigende Kosten – könnte man schnell zu dem Schluss kommen, dass ein wirksamer Datenschutz in AWS nahezu unmöglich ist. Dennoch sind die Vorteile von AWS für Unternehmen auf ihrem Weg in die Cloud zu bedeutend, um sie zu ignorieren.

Es wird immer wichtiger, dass Organisationen die richtige Datenschutzlösung finden und implementieren, um die Vorteile von AWS wirklich ausschöpfen zu können. Damit dies gelingt, benötigen sie eine Lösung, die jede der heutigen wichtigsten Herausforderungen rund um AWS-Backups gezielt adressiert.

Unternehmen sollten daher einen Blick auf Clumio werfen. Wir haben uns intensiv mit den Einschränkungen von AWS Backup befasst und eine Lösung entwickelt, die auf nativen Snapshots aufbaut und diese Herausforderungen beseitigt.

Werfen wir einen Blick darauf, wie wir das erreichen.

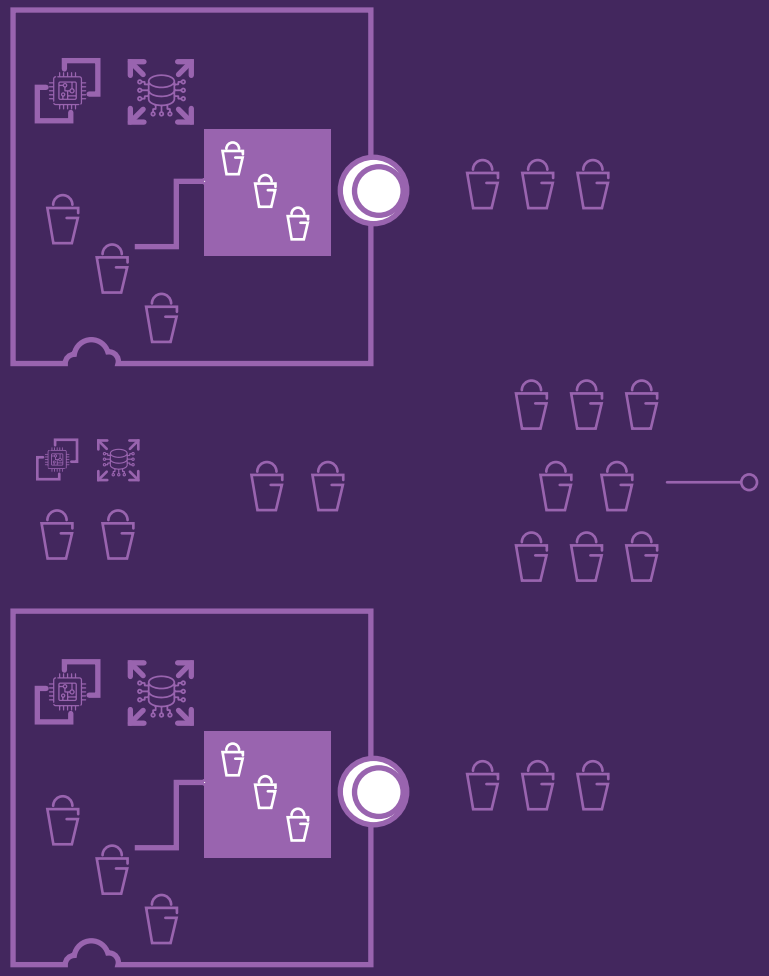
Sicherheit der Spitzenklasse

Damit Backups im Falle einer Kompromittierung der Primärdaten gültig und nutzbar sind, müssen sie außerhalb der Sicherheitszone der ursprünglichen Daten gespeichert werden. Dies wird als Air-Gap-Backup bezeichnet. Durch diese Trennung sind Backups für Hacker oder andere böswillige Akteure unerreichbar, sodass eine erfolgreiche Wiederherstellung auch nach einem Kontokompromittierung möglich bleibt.

Angesichts der zunehmenden Ransomware-Angriffe und der großen, dezentralisierten Angriffsfläche in der Cloud sollten Unternehmen besonderes Augenmerk auf die Sicherheitsarchitektur ihrer Cloud-Datenschutzlösung legen.

Die Lösung sollte Folgendes bieten:

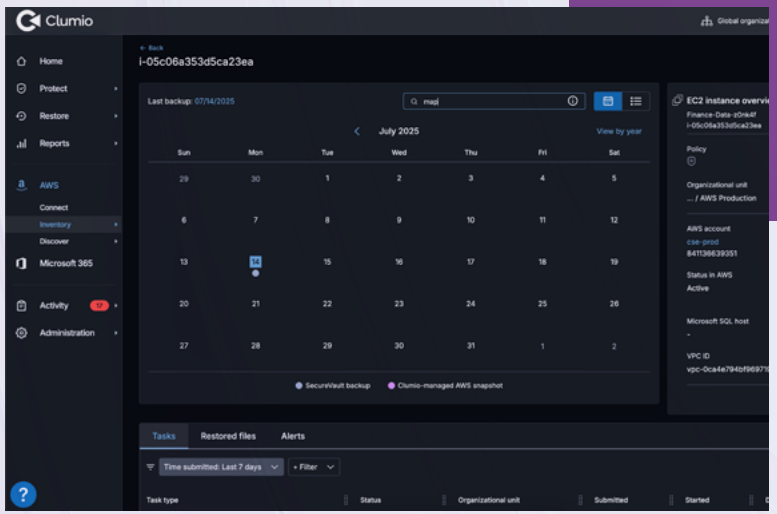
- Air-gapped Backups
- Unveränderliche Backups (immutable), sodass Sicherungskopien selbst dann nicht verändert werden können, wenn ein Angreifer irgendwie Zugriff erhält
- Keine Option zum Löschen von Backup-Daten; in Kombination mit unveränderlichen Backups wird die Datensicherung optimal geschützt
- Ende-zu-Ende-Verschlüsselung der Nutzerdaten – sowohl während der Übertragung als auch im Ruhezustand



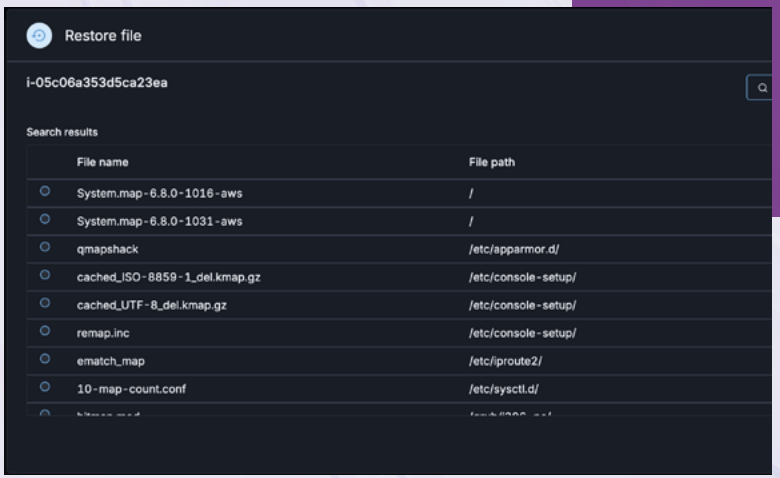
Air-Gap + Langzeitaufbewahrung
Schutz vor Ransomware und böswilligen Akteuren
Unveränderliche Backups
Kein Lösch-Button
Lifecycle-Management, das Kosteneinsparungen ermöglicht

Schnelle Wiederherstellung

Wenn eine Wiederherstellung nach einem Datenfehler notwendig ist, sollte sie schnell erfolgen können, um die Geschäftskontinuität sicherzustellen. Die richtige Datenschutzlösung muss einen schnellen Weg bieten, die benötigten Daten (Snapshots, Instanzen, Dateien, Datensätze usw.) zu finden und wiederherzustellen. So ermöglicht Clumio eine schnelle Wiederherstellung von Dateien in Amazon EC2.



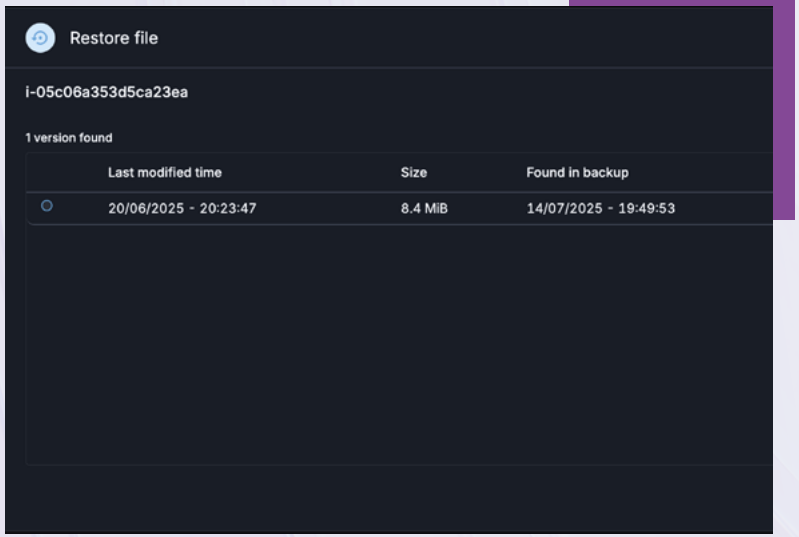
Schritt 1: Einen Suchbegriff für die Datei eingeben, die wiederhergestellt werden soll



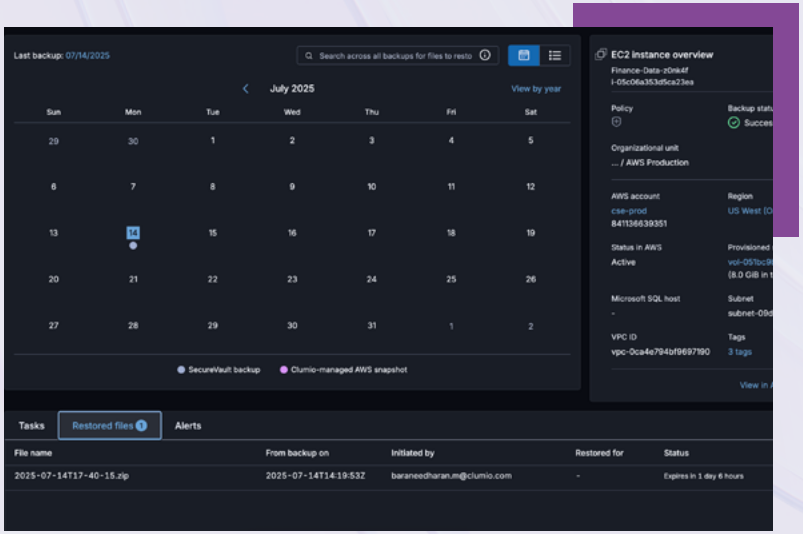
Schritt 2: Die Datei auswählen, die wiederhergestellt werden soll

Im Gegensatz zum wenig transparenten Wiederherstellungsprozess mit AWS Backup bietet Clumio eine Kalenderansicht, mit der Unternehmen effizient das gesamte Dateisystem durchsuchen können. Anstatt eine Datei erst laden oder wiederherstellen zu müssen, um dann festzustellen, ob sie die richtige ist, kann eine Organisation die benötigte Datei einfach durch Eingabe von Suchparametern finden. Der Benutzer sieht alle verfügbaren Versionen mit Zeitstempeln und kann problemlos die gewünschte Datei oder mehrere Dateien identifizieren und wiederherstellen.

Clumio verkürzt die Wiederherstellungszeit erheblich, indem es Unternehmen ermöglicht, in ihrem gesamten „Dateikistenlager“ zu suchen, ohne jede einzelne Kiste öffnen zu müssen. Dieser benutzerfreundliche, schnelle Wiederherstellungsprozess hat Clumio-Kunden geholfen, ihre durchschnittlichen Wiederherstellungszeiten von über 4 Stunden auf bis zu 10 Minuten zu reduzieren.



Schritt 3: Die gewünschte Version zum Herunterladen auswählen



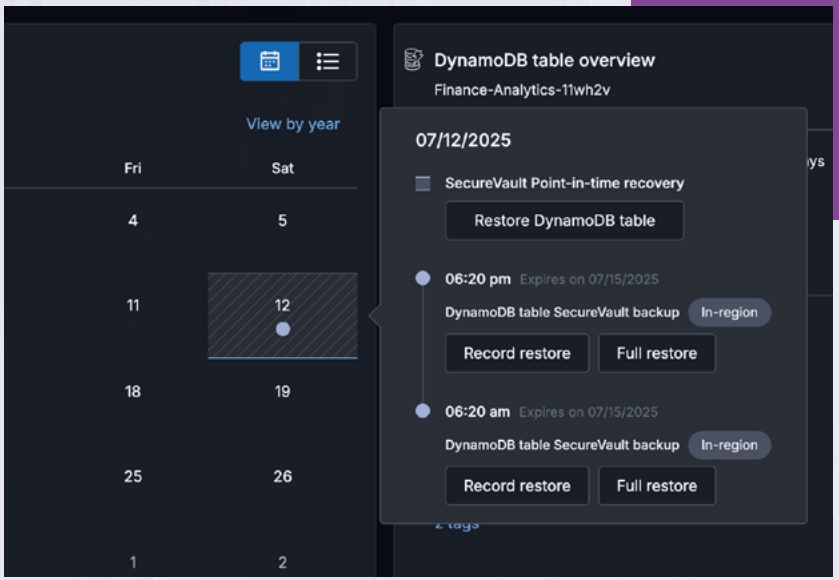
Fertig! Datei herunterladen.

Bessere Transparenz

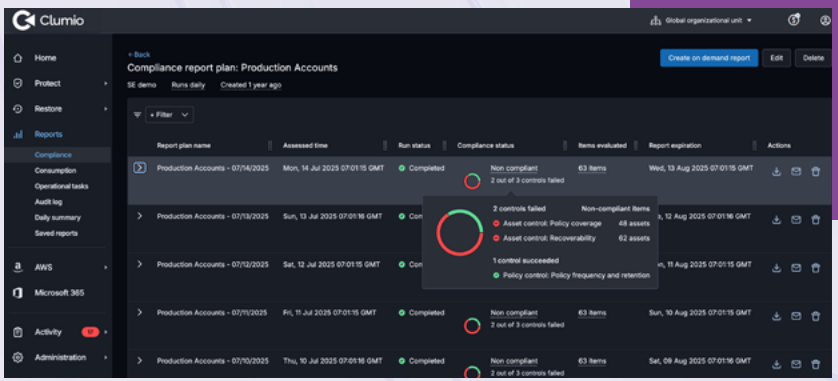
Ein zentrales Merkmal einer guten Datenschutzlösung ist die Fähigkeit, alle wichtigen Informationen über geschützte Assets klar und verständlich bereitzustellen. Wenn Benutzer eigene Berichte und Dashboards entwickeln müssen, um einen Überblick über geschützte Assets, angewandte Richtlinien, globalen kontenübergreifenden Status oder die Einhaltung von Compliance-Vorgaben zu erhalten, führt dies zwangsläufig zu Fehlern und bindet dauerhaft wertvolle Ressourcen. Stattdessen sollten solche Funktionen integraler Bestandteil der Datenschutzlösung sein.

Die Kalenderansicht in Clumio bietet ein globales Verständnis aller Snapshots und Backups, die für eine AWS-Datenquelle (EC2, EBS, RDS usw.) erstellt wurden. So können Sie problemlos eine zeitpunktbezogene Wiederherstellung der gesamten Datenquelle durchführen oder einzelne Dateien/Datensätze einsehen, um selektive Wiederherstellungen vorzunehmen.

Clumios Umgebungs-Dashboard und der Compliance-Bericht liefern in Echtzeit den Compliance-Status für ausgewählte Accounts oder die gesamte Umgebung. Dies ermöglicht es Sicherheitsteams, jederzeit die Daten-Governance im Blick zu behalten und bei Bedarf auditbereit zu sein.



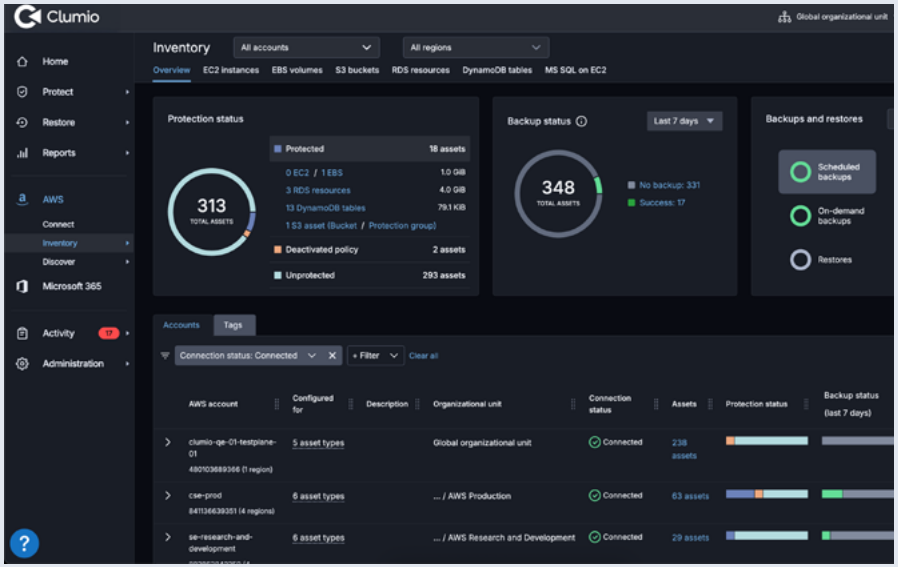
Backup-Historie in der Kalenderansicht:
Jede Sicherung schnell finden, um jederzeit eine zügige Wiederherstellung durchzuführen.



Globale Compliance-Berichte:
Eine einzige verlässliche Quelle für Audits und Compliance.

Einfacheres Management

Unternehmen sollten nach Cloud-Datenschutzlösungen suchen, die die Backup-Orchestrierung vereinfachen und automatisieren.



Die Lösung sollte ein unkompliziertes Onboarding, schnelle Backups, globale Richtlinieneinstellungen und eine einfache Wiederherstellung ermöglichen. Mit einem SaaS-Datenschutzservice wie Clumio dauert es nur etwa 10 Minuten, um AWS-Datenquellen zu schützen, und Sie erhalten gleichzeitig eine feingranulare Kontrolle über Ihre Backup- und Wiederherstellungsprozesse.

Dies vereinfacht und automatisiert tägliche Aufgaben für IT- und Betriebsteams und schafft Freiräume, damit diese sich auf das Kerngeschäft konzentrieren können.

Commvault

Instanz-wiederherstellung

Eine gesamte Instanz in ein beliebiges Konto wiederherstellen

Durchsuchen und Wiederherstellen

Das Dateisystem durchsuchen, um die gewünschte Datei wiederherzustellen

Granulare Datensatzwiederherstellung

Schema-Browser mit Wiederherstellung einzelner Datensätze per SQL-Abfrage

Globale Suche

Nach beliebigen Dateien über alle Instanzen oder Volumes hinweg suchen

Globale Richtlinien

Richtlinieneinstellungen über mehrere Konten hinweg vereinfachen

Niedrigere Gesamtbetriebskosten (TCO)

Einer der wichtigsten TCO-Vorteile von Clumio liegt in der Art und Weise, wie das Air-Gap-Verfahren implementiert wird. In einem typischen Szenario würde ein Unternehmen, das beispielsweise Snapshots im Wert von 100.000 US-Dollar in seinem AWS-Konto gespeichert hat und diese in ein „air-gapped" Konto kopieren möchte (also in ein Konto mit separaten Zugangsdaten), seine Kosten sofort auf 200.000 US-Dollar verdoppeln.

Mit Clumio ist dieser Prozess hingegen automatisch und vollständig verwaltet. Es ist kein Tiering erforderlich, um das sich der Kunde kümmern muss; alles wird automatisch übernommen, und der Kunde zahlt einfach ein leicht verständliches Preismodell pro GB. Innerhalb von nur 10 Minuten kann ein Unternehmen mit einem Klick seine Daten in einer air-gapped Umgebung sichern. Es müssen keine Skripte erstellt werden, kein Prozess verwaltet werden, und keine Spiegelkopien der Snapshots angelegt werden – was Arbeitsaufwand reduziert und die Backup-Kosten senkt.

Das Diagramm auf der nächsten Seite zeigt, dass Unternehmen durch die Nutzung eines Datenschutzservices wie Clumio, der über integrierten Air-Gap-Schutz sowie Lifecycle-Management für die langfristige Aufbewahrung verfügt, ineffiziente Backup-Methoden vermeiden können und durchschnittlich 30 % oder mehr ihrer AWS-Backup-Kosten einsparen.

Angesichts der zahlreichen weiteren Vorteile, die diese Lösung bietet, ist dies das sprichwörtliche Sahnehäubchen. Darüber hinaus unterstützt Clumio Unternehmen dabei, zu verstehen, welche Faktoren ihre Backup-Kosten antreiben. Und für Kunden, die ihre Backups einfach in einem sicheren air-gapped Vault schützen möchten, bietet Clumio die Möglichkeit, Snapshots zu geringeren Kosten als die nativen AWS-Snapshots zu migrieren.

Es ist daher wenig überraschend, dass immer mehr Unternehmen ihre AWS-Backups zu Clumio verlagern.

Der ultimative Leitfaden für AWS-Backups

Durch den Wechsel zu Clumio erhalten Sie alle Vorteile einer maßgeschneiderten Lösung – jedoch ohne die laufenden Kosten für deren Entwicklung und Wartung: keine versteckten Lizenzgebühren, einfachere Verwaltung, niedrigere Kosten als mit nativen AWS-Snapshots und bessere Berichtsmöglichkeiten.

Clumio

Bereit, das Backup für AWS zu vereinfachen?

Fordern Sie eine persönliche 1:1-Demo an:

www.clumio.com/demo

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®