IDC Link
Real-Time IDC Research® Opinion on Industry News, Trends, and Events

Commvault stellt „Resilience Ops" auf der SHIFT 2025 vor

21. November 2025

von: Phil Goodwin, Archana Venkatraman, Johnny Yu

IDC-QUICK TAKE

Es ist unbestritten, dass Resilienz – sei es in Bezug auf das Tagesgeschäft, die Daten oder die Cybersicherheit – für Unternehmen unerlässlich ist. Die Bereitstellung der erforderlichen Mitarbeiter, Prozesse und Technologien kann jedoch eine Herausforderung darstellen. Auf der Veranstaltung „Commvault SHIFT 2025", die kürzlich in New York stattgefunden hat, stellte Commvault das Konzept der „Resilience Operations" (ResOps) vor – ein Rahmenwerk, das die erforderlichen Komponenten innerhalb von Unternehmen zusammenführt.

HÖHEPUNKTE DER VERANSTALTUNG

Commvault SHIFT ist die jährliche Veranstaltung des Unternehmens, bei der die wichtigsten Ankündigungen gemacht werden. In diesem Jahr gab es einige solcher Ankündigungen, darunter:

- **„ResOps":** Obwohl es sich nicht um eine Produktankündigung handelt, hat Commvault den Begriff „ResOps" geprägt, um seine Bemühungen zur Konsolidierung der Menschen, Prozesse und Technologien zu beschreiben, die zur Verbesserung der geschäftlichen Resilienz erforderlich sind. Commvault erhebt zwar keinen Anspruch darauf, alle Elemente bereitzustellen, aber ResOps ist eine Möglichkeit für IT-Organisationen, über die Schaffung des für die Erreichung von Resilienz erforderlichen Ökosystems nachzudenken. ResOps umfasst laut Commvault die Datenerkennung und Zugriffskontrolle, die Erkennung von Anomalien und Kompromittierungsindikatoren (IoCs) sowie die saubere Wiederherstellung vertrauenswürdiger Daten.
- **Commvault Cloud Unity:** Diese Cloud-native Plattform, die nächste Generation von Commvault Cloud, steht in direktem Zusammenhang mit ResOps, da sie die Lösungen von Commvault in den Bereichen Datensicherheit, Identitätssicherheit, Governance und Wiederherstellung für Daten und Anwendungen sowohl vor Ort als auch in der Cloud vereint.
- **Synthetische Wiederherstellung:** Die Ermittlung des letzten bekannten sauberen Datenpunkts ist für die Wiederherstellung nach Cyberangriffen mit minimalem Datenverlust von entscheidender Bedeutung. Die synthetische Wiederherstellung von Commvault ist eine KI-gestützte Methode zur Kuratierung von Backups und Snapshots sowie zur Erstellung eines sicheren Wiederherstellungspunkts auf der

Grundlage der letzten bekannten sauberen Versionen einzelner Dateien und Objekte.

- **KI-gestützte Benutzeroberfläche für unternehmensweite Backup-Richtlinien:** Obwohl bereits im Rahmen von SHIFT 2023 eingeführt, wurde der KI-Agent „Arlie" des Unternehmens weiterentwickelt und bietet nun „Konversationsresilienz" durch Sprachinteraktion für agentische Automatisierung mit Arlie Advisor und Arlie Recovery.
- **Verbesserte Sicherheit:** Die Sicherheit in Commvault Cloud Unity basiert auf einer adaptiven Struktur, die sich über lokale und Cloud-Umgebungen erstreckt. Sie erhöht das Vertrauen durch Sicherheitszonen, ein gehärtetes Betriebssystem auf Linux-Basis, welches das Unternehmen als „Vault OS" bezeichnet, Zero Trust und fortschrittliche Verschlüsselung einschließlich Post-Quantum-Kryptografie (PQC).
- **Identitätsresilienz:** Commvault hat einen erweiterten Schutz für Microsoft Active Directory angekündigt. In naher Zukunft soll die Unterstützung auch auf EntraID und Okta ausgedehnt werden. Da sich Cyber-Kriminelle zunehmend darauf konzentrieren, Identitätsmanagementsysteme zu deaktivieren, um Lösegeld zu erpressen, wird die Fähigkeit, diese Systeme zu schützen und wiederherzustellen, immer wichtiger. Commvault konzentriert sich deshalb darauf, proaktive Funktionen wie Schwachstellenbewertungen und Audits hinzuzufügen, um einen klaren Überblick über die Sicherheitslage des Identitäts- und Zugriffsmanagements zu bieten.
- **Integration von Übernahmen:** Die von Commvault übernommenen Unternehmen Satori (KI-basierte Datenverwaltung und -sicherheit) und Clumio (autonome AWS-Datensicherung) sind nun als integrierte Komponenten von Commvault Cloud Unity verfügbar.

IDC-STANDPUNKT

Der Markt für Datenschutzsoftware hat sich in den letzten Jahren rasant entwickelt – angetrieben durch Cyberangriffe und in jüngerer Zeit durch KI. Obwohl weltweit mehr als 40 Anbieter auf diesem Markt tätig sind, kontrollieren die sieben größten von ihnen fast 60 % des Marktanteils. Laut IDC-Daten lag Commvault im Jahr 2024 beim Marktanteil für Datenschutzsoftware auf Platz 5. Einige dieser anderen Top-Anbieter haben sich als Anbieter von Datensicherheitslösungen positioniert, andere als KI-Anbieter oder mit anderen Varianten dieser Themen.

Wir halten die Entscheidung von Commvault, sich als Unternehmen mit dem Thema Resilienz stärker zu positionieren, für eine solide Strategie. Eine Neupositionierung ist nie einfach, und Resilienz stellt eine Erweiterung der Kernkompetenzen von Commvault dar. Das bedeutet jedoch nicht, dass das Unternehmen KI oder Datensicherheit vernachlässigt, wie die jüngsten Übernahmen und Ankündigungen für SHIFT 2025 zeigen. Durch die

Positionierung als führendes Unternehmen im Bereich ResOps hat Commvault die Möglichkeit, dieser Kategorie Form zu verleihen.

Erweiterung in alle Richtungen

Angesichts zunehmender Komplexität, Risiken und Kundenerwartungen ist Resilienz für Unternehmen zu einer strategischen Priorität geworden. Daher konzentrieren sich viele Technologieanbieter – darunter Infrastruktur-, Sicherheits- und Überwachungsanbieter – auf die Verbesserung der digitalen Resilienz. Dies geschieht jedoch in erster Linie aus der Perspektive der Erkennung und Identifizierung. Mithilfe von Ursachenanalysen werden Teams dazu angehalten, schnell Maßnahmen zu ergreifen, anstatt nach der Nadel im Heuhaufen zu suchen. Die Anbieter fordern Unternehmen dazu auf, Resilienz auf ihrem Weg zu berücksichtigen und sich an Signalen zu orientieren.

Mit seiner ResOps-Vision strebt Commvault danach, seine Resilienz-Lösungen zu erweitern: einerseits, indem es mit der kürzlich erfolgten Übernahme von Satori Datensicherheitsfunktionen hinzufügt (z. B. Datenerkennung und -klassifizierung, Überwachung und Durchsetzung von Zugriffsrichtlinien), und andererseits, indem es mehrere aufeinander aufbauende Ebenen hinzufügt. Ein Beispiel hierfür sind die Aktualisierungen des Threat-Scan-Monitors zur Identifizierung von Risiken in geschützten Daten. Die synthetische Wiederherstellung identifiziert die neuesten sauberen Daten für die Wiederherstellung auf Datei-, Objekt- oder VM-Ebene. Schließlich bietet die Cleanroom-Wiederherstellung einen sicheren Raum, um Tests und Datenvalidierungen zu automatisieren, bevor die wiederhergestellten Daten in die Produktion zurückgeführt werden. All dies zeigt einen vollständigen, modernen End-to-End-Wiederherstellungsworkflow in Aktion. Damit wird Resilienz Realität.

ResOps ist für Commvault eine doppelte Chance:

- Befähigung traditioneller Käufer im Bereich IT-Administration, um einen wirksamen Beitrag zu den Resilienzstrategien von Unternehmen zu leisten. Die auf ResOps ausgerichteten Technologien von Commvault ermöglichen es seinen Anwendern, jederzeit ihre Bereitschaft zur Wiederherstellung nach einem Vorfall unter Beweis zu stellen und durch die Reduzierung von Wiederherstellungszeiten, Kosten oder Fehlern quantifizierbares Vertrauen in die Geschäftskontinuität zu schaffen.
- Schaffung von Synergien mit Anbietern von Beobachtbarkeit, Sicherheit und Infrastruktur, um eine umfassende, kontinuierliche Resilienz für echte ResOps zu erreichen. Dies kann frühzeitige Einblicke in digitale Abläufe bringen, um die Produkt-Roadmap für Commvault zu steuern und gleichzeitig Teil eines strategischen Sicherheits-Ökosystems zu sein.

Dies ist jedoch nicht ohne Risiko, da der Erfolg davon abhängt, ob IT-Organisationen bereit sind, den Begriff zu übernehmen und als Kategorie zu akzeptieren. Es braucht Zeit, bis sich der Markt eines neuen Begriffs bewusst wird, und Commvault wird Geduld und Ausdauer benötigen, bis er sich durchsetzt.

Verwirrung und Unklarheiten könnten ebenfalls zu Rückschlägen führen. IDC ist der Ansicht, dass Commvault seinen Kunden und Partnern gegenüber betonen sollte, dass „ResOps“ keine disruptiven betrieblichen Veränderungen für ihre Unternehmen bedeutet. Stattdessen sollte das Unternehmen hervorheben, wie es einige der Lücken in der betrieblichen Resilienz schließen und in bestehende Frameworks integriert werden kann, um die Resilienz auszubauen. Zu diesem Zweck muss Commvault einen kohärenten Prozess der Reifegradentwicklung für ResOps ausarbeiten, der den klaren Mehrwert hervorhebt, den seine Kernnutzer im bestehenden Resilienz-Framework ihrer Unternehmen generieren.

Dennoch sind wir der Meinung, dass ResOps bei Kunden Anklang finden kann, da es prägnant ist und starke Auswirkungen sowie einen hohen operativen Wert hat.

Es ist auch wichtig zu betonen, dass die grundlegende Umstellung von Commvault auf SaaS vor fünf Jahren (jetzt Commvault Cloud Unity) einen Wendepunkt für das Unternehmen darstellte und den Grundstein für ResOps legte. Damit verfügt der Anbieter nun über die richtige Grundlage, um neue, auf Resilienz ausgerichtete Innovationen zu entwickeln und neu erworbene Technologien schnell zu integrieren, um seiner ResOps-Vision Gewicht zu verleihen.

Abgedeckte Abonnements:
Logistik und Schutz von Cloud-Daten, Europäische Strategien zur Verwaltung von Cloud-Daten