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

Commvault présente « Resilience Ops » au SHIFT 2025

Novembre 21, 2025

Par : Phil Goodwin, Archana Venkatraman, Johnny Yu

L'AVIS D'IDC

Personne ne conteste le fait que la résilience - qu'il s'agisse de l'entreprise, des données ou de la cyber - est un impératif organisationnel, et que la mise en place des personnes, des processus et des technologies nécessaires peut s'avérer difficile. Lors de son récent événement Commvault SHIFT, Commvault a présenté le concept de « Resilience Operations » ou « ResOps » comme un cadre permettant de rassembler les éléments nécessaires au sein des organisations.

FAITS MARQUANTS DE L'EVENEMENT

Commvault SHIFT est l'événement annuel au cours duquel l'entreprise fait ses annonces les plus importantes. Voici quelques-unes des annonces faites lors de l'événement de cette année :

- **« ResOps » :** bien qu'il ne s'agisse pas d'une annonce de produit, Commvault a inventé le terme *ResOps* pour décrire ses efforts visant à consolider les personnes, les processus et les technologies nécessaires pour améliorer la résilience de l'entreprise. Bien que Commvault ne prétende pas fournir tous les éléments, ResOps est une façon pour les organisations informatiques de penser à la création de l'écosystème nécessaire pour atteindre la résilience. ResOps, tel que décrit par Commvault, comprend la découverte des données et le contrôle d'accès, la détection des anomalies et des indicateurs de compromission (IdC), et la récupération propre des données de confiance.
- **Commvault Cloud Unity :** cette plateforme cloud-native, la prochaine génération de Commvault Cloud, est directement liée à ResOps car elle unifie les solutions de Commvault autour de la sécurité des données, de la sécurité des identités, de la gouvernance et de la restauration des données et des applications, qu'elles soient sur site ou dans le cloud.
- **Récupération synthétique :** déterminer le dernier point de données propre connu est essentiel pour se remettre d'une cyberattaque avec une perte de données minimale. La récupération synthétique de Commvault est une méthode basée sur l'intelligence artificielle qui permet d'analyser les sauvegardes et les snapshots et d'assembler un point de récupération sûr basé sur les dernières versions connues de fichiers et d'objets individuels.

- **Interface utilisateur pilotée par l'IA pour les politiques de sauvegarde à l'échelle de l'entreprise :** bien que présenté lors du SHIFT 2023, « Arlie », l'agent IA de l'entreprise, a été amélioré pour offrir une « résilience conversationnelle » utilisant l'interaction vocale pour l'automatisation agentique Arlie Advisor et Arlie Recovery.
- **Sécurité renforcée : l**a sécurité de Commvault Cloud Unity est basée sur une structure adaptative entre les environnements sur site et cloud. La solution renforce la confiance à l'aide de zones de sécurité, d'un système d'exploitation renforcé basé sur Linux que l'entreprise a baptisé « vault OS », une architecture « zero-trust » (à vérification systématique) et un chiffrement avancé comprenant la science du chiffrement post-quantique (PQC).
- **Résilience de l'identité :** Commvault a annoncé une protection élargie pour Microsoft Active Directory avec la prise en charge d'EntraID et d'Okta dans un avenir proche. Les cyber-attaquants s'efforcent de plus en plus de désactiver les systèmes de gestion des identités afin d'obtenir une rançon, d'où l'importance croissante de la capacité à protéger et à récupérer ces systèmes. Commvault se concentre sur l'ajout de fonctionnalités proactives telles que l'évaluation des vulnérabilités et l'audit afin d'offrir une vision claire de la posture de sécurité de la gestion des identités et des accès.
- **Intégration des acquisitions : l**es acquisitions par Commvault de Satori (gouvernance et sécurité des données IA) et de Clumio (protection autonome des données AWS) apparaissent désormais comme des composants intégrés de Commvault Cloud Unity.

LE POINT DE VUE D'IDC

Le marché des logiciels de protection des données évolue rapidement depuis plusieurs années, sous l'impulsion des cyberattaques et, plus récemment, de l'IA. Bien que plus de 40 fournisseurs participent à ce marché à l'échelle mondiale, les 7 principaux fournisseurs contrôlent près de 60 % des parts de marché (selon les données d'IDC, Commvault était le numéro 5 en termes de parts de marché pour les logiciels de protection des données en 2024). Certains de ces autres grands fournisseurs se sont adaptés pour se positionner en tant que fournisseurs de sécurité des données, d'autres en tant que fournisseurs d'IA, ainsi que d'autres variations sur ces thèmes.

Nous pensons que la décision de Commvault de mettre l'accent sur la résilience en tant que positionnement de l'entreprise est une stratégie solide. Le repositionnement n'est pas facile, et la résilience est un prolongement de la compétence principale de Commvault. En outre, cela ne signifie pas que l'entreprise renonce à l'IA ou à la sécurité des données, comme l'illustrent les récentes acquisitions et les annonces faites lors du

SHIFT 2025. En s'imposant comme leader en matière de ResOps, Commvault a l'opportunité de définir cette catégorie.

Déplacement vers la gauche mais aussi prolongement vers la droite

Face à la complexité croissante, aux risques et aux attentes des clients, la résilience est devenue une priorité stratégique pour les organisations. Par conséquent, de nombreux fournisseurs de technologies (fournisseurs d'infrastructures, de sécurité et de surveillance) se concentrent sur l'amélioration de la résilience numérique. Mais c'est principalement du point de vue de la détection et de l'identification. Ces plateformes orientent les équipes vers l'analyse des causes profondes afin qu'elles prennent des mesures rapides au lieu de chercher une aiguille dans une botte de foin. Ces fournisseurs incitent les organisations à prendre en compte la résilience dans leur parcours et à se laisser guider par les signaux.

Avec sa vision ResOps, Commvault cherche à étendre ses solutions de résilience vers la gauche en ajoutant des capacités de sécurité des données grâce à sa récente acquisition de Satori (par exemple, la découverte et la classification des données, la surveillance et l'application des politiques d'accès), ainsi qu'à étendre vers la droite avec des couches multiples qui s'appuient les unes sur les autres. Les mises à jour du moniteur Threat Scan, qui permet d'identifier les risques dans les données protégées, en sont un exemple. Synthetic Recovery identifie les dernières données propres à récupérer au niveau du fichier, de l'objet ou de la machine virtuelle. Enfin, Cleanroom Recovery offre un espace sécurisé pour automatiser les tests et la validation des données avant de renvoyer les données récupérées vers la production. Cela montre un flux de travail de récupération moderne complet de bout en bout en action. La résilience devient ainsi une réalité.

ResOps représente une double opportunité pour Commvault :

- Permettre à ses acheteurs traditionnels dans le domaine de l'administration informatique de contribuer efficacement aux stratégies de résilience d'une organisation. Les technologies ResOps de Commvault permettent à ses utilisateurs de prouver en permanence qu'ils sont prêts à se remettre d'un incident et de fournir une confiance quantifiable dans la continuité de l'activité en réduisant le temps de récupération, les coûts ou les erreurs.
- Synergie avec les fournisseurs de solutions d'observabilité, de sécurité et d'infrastructure pour une approche plus cohérente autour d'une résilience complète et continue pour un véritable ResOps. Cela peut apporter des informations préliminaires sur les opérations numériques pour guider la feuille de route des produits de Commvault tout en faisant partie d'un écosystème de sécurité stratégique.

Ce n'est toutefois pas sans risque, car son succès dépend de la volonté des organisations informatiques d'adopter le terme ResOps et de l'accepter en tant que catégorie. Il faut du temps pour que le marché prenne conscience d'un nouveau terme, et Commvault devra faire preuve de patience et de persévérance pour y parvenir.

La confusion et l'ambiguïté pourraient également représenter des obstacles. IDC pense que Commvault devrait insister auprès de ses clients et partenaires sur le fait que « ResOps » n'implique pas un changement opérationnel perturbateur pour leurs organisations. Au contraire, l'entreprise devrait souligner comment ce concept peut combler certaines lacunes en matière de résilience opérationnelle et être ajouté aux cadres existants pour étendre la résilience à droite. Pour cela, Commvault doit développer un parcours cohérent de maturité ResOps en soulignant la valeur claire que ses utilisateurs principaux apportent au cadre de résilience existant de leur organisation.

Néanmoins, nous pensons que ResOps devrait susciter l'intérêt des clients, car il est concis, avec une valeur opérationnelle et des avantages puissants.

Il est également important de souligner que le passage de Commvault au SaaS il y a cinq ans (aujourd'hui Commvault Cloud Unity) a été pour l'entreprise un tournant à l'origine de ResOps. Cela a donné à l'éditeur la bonne base pour construire des innovations axées sur la résilience et intégrer rapidement les technologies nouvellement acquises afin de donner du poids à sa vision ResOps.

Abonnements couverts :
Logistique et protection des données dans le cloud, Stratégies européennes de gestion des données dans le cloud