LES CAHIERS THÉMATIQUES
DE STORDATA

Le data management #4

Rubrik Security Cloud

La sécurité by design des systèmes de sauvegarde, en environnements hybrides et Multicloud

Stordata

éditorial

Joël Thouvenin
Directeur commercial

Quel métier que celui de la sauvegarde.

C'est une affaire de spécialistes, n'est-ce pas ? Les administrateurs ne diront pas le contraire. Mais où sont-ils ces administrateurs sauvegarde, prêts à passer des heures à rechercher la cause d'un incident ? De moins en moins nombreux, en partie parce qu'il n'existe (toujours!) pas de formation pour ces tâches hautement complexes, les experts du backup ne cachent pas la réalité de la désaffection. Après tout, la sauvegarde est d'abord une assurance, un mal nécessaire qu'on préférerait confier à d'autres. Le processus a notamment le chic pour mettre en évidence le moindre problème de configuration, le plus petit grain de sable dans le rouage délicat de l'infrastructure, ce qui peut devenir crispant, à la longue. Nous en convenons.

En conséquence de quoi, les rangs se vident et les DSI s'interrogent. N'y a-t-il donc pas plus simple ? Plus rapide ? Plus efficace ?

La réponse est évidemment oui, parce que les générations de technologies se suivent tout en ayant le bon goût de ne pas se ressembler. La déferlante de l'hyperconvergence (et sa simplicité d'acquisition et d'exploitation) a donné naissance à de nouvelles solutions de sauvegarde particulièrement ingénieuses.

Rubrik Security Cloud fait partie de cette nouvelle génération de solutions tout en un, nourries à l'hyperconvergence. Un véritable séjour all inclusive, un peu comme sait en concevoir le secteur du tourisme. L'analogie est assez juste après tout puisque Rubrik a pensé l'expérience de la défense de la donnée comme un beau voyage d'agrément, depuis sa protection zero trust jusqu'à sa restauration ultra-rapide en passant par une surveillance intégrée qui manquait jusque-là.

Entre simplicité, réactivité et sécurité, Rubrik fait un sans-faute en s'adressant aux équipes fortement sensibilisées à la cyberdéfense, qui cherchent à transformer leurs pratiques et leur organisation.

Réflexions préliminaires et arbitrages

Les sauvegardes, nouveau terrain de jeu des pirates

Puisque la sauvegarde est le dernier recours des entreprises contre les conséquences d'une cyberattaque réussie (en dehors du coup de canif porté au contrat moral), il n'en fallait pas plus pour que le domaine devienne le nouvel eldorado de la piraterie. Plus de 20 % des attaques par ransomwares ciblent dorénavant les sauvegardes, par ricochet ou directement, qu'elles soient sur un serveur ou dans le Cloud.

S'il existe plusieurs mesures pour se prémunir en partie du risque, force est de constater que les entreprises ne sont encore ni bien préparées ni bien informées sur ce type particulier de menace, ignorant souvent que leur système de sauvegarde, indispensable acteur de leur PRA, n'est pas toujours sécurisé by design.

Le secteur a toujours décorrélé la sauvegarde et donc la protection de la donnée, de la sécurité. Les mécanismes diffèrent, c'est vrai. À la première, vont les politiques, inventaire, hiérarchisation, stockage secondaire et tertiaire, PRA/PCA et leurs tests. À la seconde, les stratégies cyberdéfense et leur cohorte de réglementations, sensibilisation et formation, mécanismes d'intelligence artificielle, jusqu'à la cyber-résilience dont la sauvegarde, ironiquement, est une des clés.

Un biais qui se traduit par une organisation en interne divisée : d'un côté, l'administrateur de sauvegarde, de l'autre, le RSSI, chacun fort de ses technologies, de ses missions, de ses objectifs et de son langage.

Une sauvegarde corrompue signifie donc qu'un mécanisme de protection de la donnée sauvegardée exige au moins le même degré de sécurité que la donnée elle-même. Mais jusqu'où ira-t-on, se demande-t-on ? Nous ne le savons pas hélas. Mais nous savons que des éditeurs comme Rubrik ont très tôt perçu cette évolution du risque et du besoin de sécurité au cœur même du processus de sauvegarde et du patrimoine sauvegardé.

Cloud or not Cloud ?

Rubrik Security Cloud sécurise les données de l'entreprise (applications, fichiers, utilisateurs), où qu'elles se trouvent, confirmant ainsi l'appétence des entreprises pour l'usage du Cloud, qu'il s'agisse d'hybridation et de Multicloud.

Poursuivant le raisonnement, l'éditeur privilégie la flexibilité du cloud public pour la protection des applications d'entreprise, mais également la possibilité d'exploiter rapidement des instances de test/dev à partir d'un seul et unique point de contrôle.

L'archivage dans le Cloud est à ce titre également proposé, d'autant que l'éditeur a su conclure d'intéressants partenariats avec les 3 grandes plateformes se partageant le marché.

La console d'administration, en charge notamment de l'analyse des flux chiffrés, est elle aussi, en toute logique, hébergée dans le Cloud.

Mais qu'en est-il de l'appliance ? Rubrik propose son appliance selon deux modes de consommation. Pour les plus fervents admirateurs du modèle Cloud, une version SaaS est disponible, associant machines virtuelles et stockage virtuel.

Stordata en revanche dirige sa préférence vers la seconde option, une appliance physique installée dans les locaux de l'entreprise, et encore très souvent plébiscitée des équipes internes. Proposant jusqu'à 100 tera de stockage secondaire (extensible en cluster), cette machine physique déplace les données les plus anciennes vers tout type de stockage froid et notamment les plus souverains, au besoin. Les données Cloud sauvegardées sont, elles, stockées dans le Cloud public.

Rubrik Security Cloud, la surveillance musclée au service d'une sauvegarde réputée sûre

1 Protection des données avec des sauvegardes immuables, un air-gap logique, et un contrôle des accès aux comptes

• Rubrik a mis l'accent sur une appliance abritant une couche logicielle maison conçue pour être extrêmement sécurisée, donc particulièrement difficile à attaquer, grâce à un file system immuable.

Rubrik est notamment porté par d'anciens ingénieurs venus de l'équipe à l'origine du Google file system.

• Le Role Based Access Control (RBAC) organise soigneusement la gestion des identités et l'examen des droits d'accès. Si l'on retrouve la désormais traditionnelle double authentification (MFA), embarquée par conception (by design pour qui préfère l'expression américaine), Rubrik Security Cloud prend en compte le risque d'ingénierie sociale dans tous ses aspects. Ainsi, même un administrateur dûment authentifié ne pourra pas supprimer de fichier à la volée sans requérir une seconde autorisation, voire se soumettre à une double action (à l'instar de l'ouverture de certains coffres en banque). Même la corbeille Rubrik reste encore accessible pendant un certain temps, afin de récupérer des éléments supprimés tels que des sauvegardes.

> **" Rubrik est notamment porté par d'anciens ingénieurs venus de l'équipe à l'origine du Google file system. "**

Automatisation de milliers de tâches

Parmi les nombreux avantages remarquables de Rubrik Security Cloud, la simplicité d'utilisation se constate à travers le petit nombre de politiques de sauvegarde nécessaires, applicables in fine. L'automatisation s'applique autant à la fréquence des sauvegardes, qu'à la rétention, la réplication ou l'archivage, on-premise comme dans le Cloud.

En somme, Rubrik s'affranchit du monde UNIX, repart entièrement d'une feuille blanche, gardant à l'esprit l'expérience utilisateur comme fil rouge de sa conception.

2 Monitoring en continu des données pour détecter un ransomware, une exposition des données ou des indicateurs de compromission

• Puisque les sauvegardes sont désormais une cible de choix, Rubrik introduit la détection des comportements anormaux et des signatures. La solution alerte les administrateurs au-delà d'un certain taux de modification, selon paramétrage.

• Très pertinente au regard du RGPD et des exigences de conformité notamment bancaire, la visibilité des données sensibles (personnelles ou non), propose un vrai détail du patrimoine sauvegardé, augmentant d'autant la vitesse d'évaluation du risque encouru et des mesures à prendre en cas de compromission.

• La détection des compromissions permet en outre de dater une éventuelle infiltration et de verrouiller les sauvegardes antérieures et sûres. En cas d'urgence, les équipes disposent d'un spectre d'informations plus large pour restaurer en confiance. D'une certaine manière, Rubrik renseigne sur la restaurabilité des fichiers sauvegardés, un vrai gain de temps.

Fédérer les équipes autour d'une même solution

En matière de sécurité, Rubrik Security Cloud répond à 3 des questions les plus importantes : où se situe la menace ? quand s'est-elle présentée ? à quoi correspond-elle ? (La réponse au comment étant généralement à la charge d'un support comme sait le proposer Stordata).

En d'autres termes, cette solution recrée du lien entre les équipes backup et les équipes sécurité, en les dotant d'un niveau égal d'informations et en contribuant à renforcer le rôle d'alerte des administrateurs sauvegarde. Ce niveau de complémentarité entre protection et sécurité est tout à fait inédit.

Notion d'isolation logique

L'isolation logique ou air-gap logique ne signifie pas une déconnexion des systèmes mais bien l'impossibilité pour un assaillant de découvrir et d'accéder aux sauvegardes, comme d'y toucher, notamment en tentant de les chiffrer.

Le système de fichiers de type « append-only » de Rubrik n'autorise que l'ajout de nouveaux fichiers, ceux déjà présents étant incorruptibles, car immuables.

RAPPEL **Rubrik Security Cloud opère la surveillance des données quand elles sont exposées, mais elle n'inspecte pas les portes d'entrées du réseau. La solution est ainsi complémentaire aux cartographies de type EASM, mais elle n'affranchit pas de pentests réguliers (voire en continu).**

Rubrik Security Cloud (suite)

3 Restauration de manière granulaire des apps, fichiers ou utilisateurs en prémunissant l'entreprise d'une réinfection du malware

La restauration des fichiers fait sans aucun doute partie des points forts de Rubrik Security Cloud, avec des RTO proches de zéro.

- D'une part, dans les cas les plus courants, comme la suppression par mégarde d'un composant en production, il est très simple de lancer une recherche sur l'environnement de sauvegarde et de repérer jusqu'au moindre fichier utile. La grande originalité de la solution réside dans sa capacité à autoriser le redémarrage directement depuis l'appliance, d'une machine virtuelle par exemple, sans la nécessité d'une restauration immédiate.
- D'autre part, l'évaluation du degré de restaurabilité des sauvegardes permet de déterminer avec précision le point de reprise le plus conforme, rapidement. Les temps de restauration indiqués (et testés) d'environnements entiers sont de l'ordre de quelques heures, parfois moins, contre plusieurs jours ou plusieurs semaines auparavant.

Cas d'usages

Rationalisation et simplicité

La mutualisation des systèmes d'information, dans le cadre de groupements de collectivités ou de regroupements d'hôpitaux, revient à attribuer à une seule DSI la gestion de matériels et solutions hétéroclites et souvent vieillissants. Les sauvegardes deviennent instables, conduisant à de nombreux incidents.

La taille souvent réduite de l'équipe IT en collectivités territoriales conforte le besoin de rationaliser les solutions et d'aller vers plus de simplicité.

Modernité et transformation

Les grandes entreprises sont également victimes de l'empilement de solutions. La plupart des grandes DSI ayant largement finalisé leur mue vers le Cloud ou du moins vers une transformation radicale de leurs méthodes, elles attendent de leurs outils une conception moderne, sans couverture démesurée mais adaptée aux technologies qu'elles ont introduites, comme la sauvegarde des ressources virtuelles, dans le Cloud ou On premise, évidemment.

Intégration et assurance

Pour garantir aux utilisateurs la disponibilité d'applications critiques, fonctionnant en temps réel, les sauvegardes comme leur restauration doivent être extrêmement contenues.

Les environnements virtualisés profitent de l'étroite intégration de Rubrik à VMware, mais aussi avec les constructeurs Nutanix, Pure Storage et NetApp.

Notions de retour sur investissement

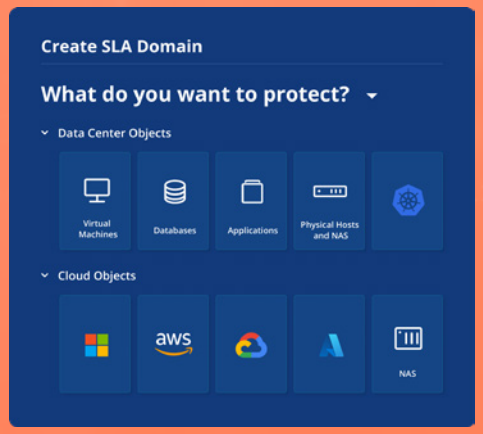
Nous ne l'apprendrons à personne, les solutions vieillissantes finissent par coûter cher une fois le contrat de maintenance arrivé à échéance. Toutefois, on rappellera utilement que la sauvegarde reste une assurance, et que les dépenses qu'elle engendre doivent être observées à l'aune du coût d'un sinistre.

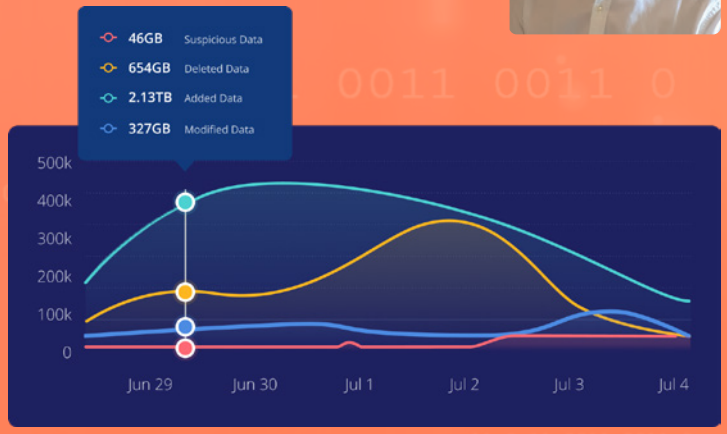
Cela dit, la baisse du coût de possession avec Rubrik est tout à fait remarquable, dès lors qu'on ne monopolise plus des équipes entières sur des processus longs et complexes. Et **même s'il n'est pas aisé de chiffrer le gain, des temps de gestion réduits de plus de 50 % ne peuvent qu'alléger un budget** que l'on sait toujours contraint.

L'avis de l'expert Stordata

Patrick DUFOUR
Directeur Stratégie et Alliance

Stordata a longuement investigué cette impressionnante solution Rubrik Security Cloud avant de s'autoriser à la proposer. De bout en bout, il aura fallu une année, d'une part pour réaliser l'indispensable POC et d'autre part, une fois la décision prise, pour former et certifier l'ensemble des collaborateurs concernés.





Cette équipe Stordata est composée d'avant-vente expert(e)s de la sauvegarde, de chargé(e)s du *Professional Services* avec une forte expertise dans le déploiement des infrastructures de sauvegarde et de responsables du support client. Il s'agissait pour les uns et les autres d'en comprendre toutes les possibilités, d'observer les conditions de déploiement et d'évaluer la qualité des outils à disposition. Nous avons tenu également à vérifier la réalité de l'accompagnement de l'éditeur, qui a fini de nous convaincre.

Le temps des certifications venu, nous avons choisi de faire suivre le cursus de formation à plus de collaborateurs que demandés par notre partenaire Rubrik, et ce à tous les niveaux, vente, service et support. Le support en particulier a très nettement renforcé ses connaissances et ses compétences sur Rubrik Security Cloud afin de pouvoir intervenir dès les premiers instants de la relation avec nos clients, ainsi que nous l'avons toujours conçu.

Rubrik Security Cloud est une solution très puissante et son concept d'appliance, spécifique à Rubrik, simplifie drastiquement la vie de l'entreprise qui en fait l'acquisition. Prêt à l'emploi, dotée d'une interface graphique moderne, exploitant pleinement tous les bénéfices du contexte hyperconvergé, Rubrik Security Cloud répond en tous points à l'idée que l'on se fait de l'innovation numérique aujourd'hui.

Rubrik Security Cloud

Résilience des données

- Protection des données Zero Trust
- Cloud Data Protection
- Microsoft 365 Protection

Observabilité des données

- Surveillance et enquête sur les attaques de ransomware
- Identification des données sensibles
- Chasse aux menaces
- Centre de commande pour la sécurité des données

Récupération des données

- Endiguement des menaces
- Restauration massive
- Restauration orchestrée des applications

Stordata

Pour déployer Rubrik Security Cloud en entreprise, Stordata procède toujours, en premier lieu, à l'évaluation du plan de sauvegarde de ses clients.

Bâti sur une précédente solution, il peut parfois demander à être rénové et le volume de machines et de bases de données concerné conditionne le temps d'étude. L'éventuelle refonte d'un plan de sauvegarde doit donc être considérée.

Le déploiement de la solution Rubrik Security Cloud requiert en outre l'établissement de spécifications détaillées. Rubrik livre une solution parfaitement mesurée (sizée) aux besoins en production tels qu'ils apparaissent dans les informations recueillies.

Puis la phase d'installation, relativement courte effectivement avec Rubrik Security Cloud, est suivie d'une phase de tests. Enfin vient la phase de recette, dont l'extrême importance s'illustre par la mise en évidence, à ce stade, de possibles points d'achoppement jusque-là inconnus. Une nouvelle recette clôture les ajustements nécessaires.

Stordata peut également simuler des pannes à la demande, pour une observation intégrale.

Enfin, le support Stordata délivre des analyses des pannes et des incidents éventuels et accompagne ses clients dans leur processus de remédiation.

En partenariat avec : rubrik

Agence Île-de-France & Nord
28, rue Saint-Honoré - 78000 Versailles
Tél. : +33 1 30 21 42 42

Agence Sud-Est
28, rue Louis Guérin - 69100 Villeurbanne
Tél. : +33 4 78 48 09 47

Agence Sud-Ouest
6, rue Maurice Caunes - 31200 Toulouse
Tél. : +33 5 34 50 49 00

Agence Méditerranée
Tél. : +33 5 34 50 49 00

Agence Ouest
34, quai Magellan - 44000 Nantes
Tél : +33 2 28 08 09 93

Agence Est
9, rue Icare - 67960 Entzheim
Tél. : +33 3 88 76 47 64

www.stordata.fr

Stordata
vos données, notre engagement