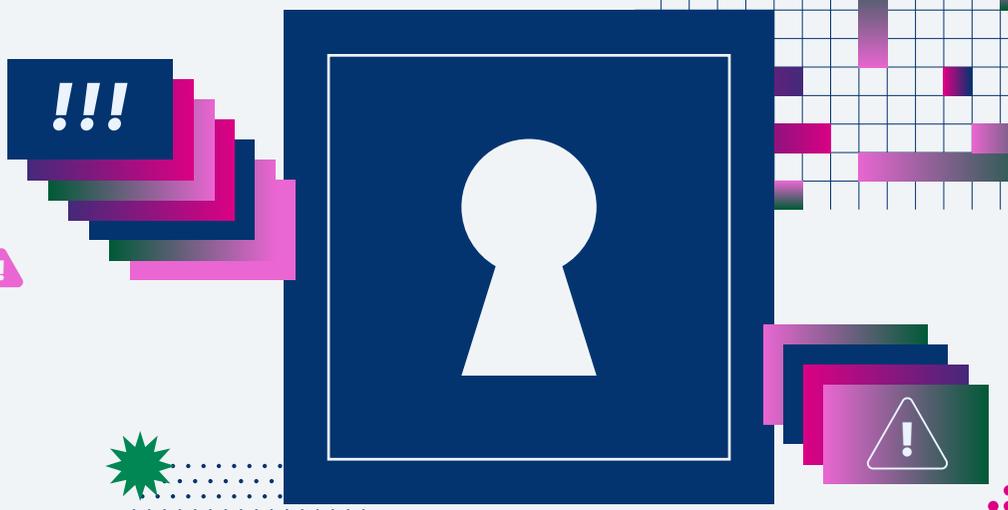


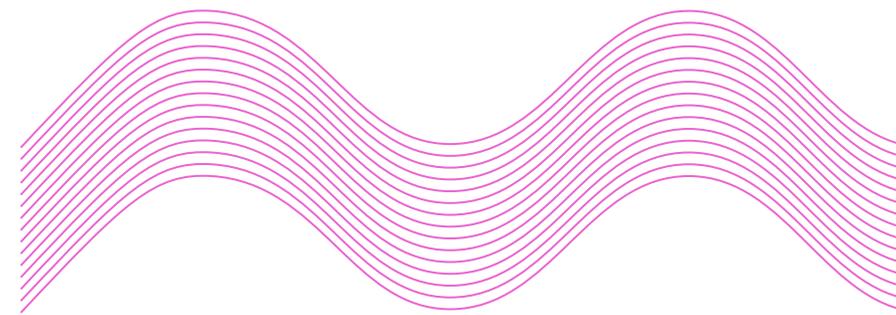


Cyber-résilience : 5 clés pour faire face à l'explosion des données non structurées

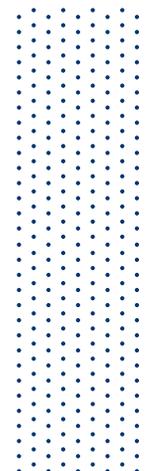
Zoom sur les lacunes des solutions d'ancienne génération et les fonctionnalités incontournables à prioriser



SOMMAIRE



LES VOLUMES DE DONNÉES NON STRUCTURÉES EXPLOSENT	3
LES CINQ INDISPENSABLES D'UNE SOLUTION DE PROTECTION DES DONNÉES NON STRUCTURÉES.....	5
Conjuguer protection et performance sur des pétaoctets de données non structurées	5
Visibilité à 360° sur l'ensemble de vos données non structurées	6
Une détection des anomalies garante de la sécurité des données à grande échelle	7
Visibilité et classification des données sensibles	8
Restauration granulaire et efficace des données	9
MODERNISEZ VOTRE PROTECTION DES DONNÉES NON STRUCTURÉES.....	10



Rubrik (NYSE: RBRK) s'est donné pour mission de sécuriser les données du monde entier. Au travers de la solution Zero Trust Data Security™, nous aidons les entreprises à renforcer leur résilience face aux cyberattaques, aux menaces internes et aux perturbations opérationnelles. Rubrik Security Cloud s'appuie sur le machine learning pour protéger les données sur l'ensemble des applications on-prem, cloud et SaaS. Intégrité, disponibilité à toute épreuve, surveillance des risques et des menaces, restauration en cas d'attaque... nous agissons sur tous les fronts de la protection et de la préservation de vos données.

Pour en savoir plus, rendez-vous sur notre site www.rubrik.com/fr et suivez notre compte [@rubrikinc](https://twitter.com/rubrikinc) sur X (anciennement Twitter) et [Rubrik](https://www.linkedin.com/company/rubrik) sur LinkedIn.

Rubrik est une marque déposée de Rubrik, Inc. Tous les noms de sociétés, noms de produits et autres noms similaires figurant dans le présent document sont des marques déposées ou des marques commerciales de la société concernée.

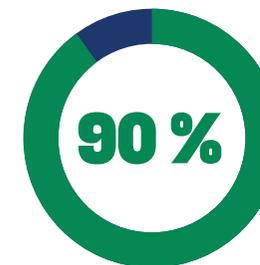
LES VOLUMES DE DONNÉES NON STRUCTURÉES EXPLOSENT

On assiste actuellement à une véritable explosion des données non structurées, à savoir les données sortant du champ des outils data conventionnels comme les bases de données relationnelles. Selon le cabinet d'études IDC, ces données non structurées représentent aujourd'hui 90 % de la datasphère mondiale. Mais le plus surprenant, c'est qu'un quart des entreprises admettent être dépassées par cette prolifération¹. Un constat d'autant plus inquiétant que les données non structurées renferment une multitude d'informations sensibles : propriété intellectuelle (PI), données à caractère personnel (DCP), travaux de recherche, etc.

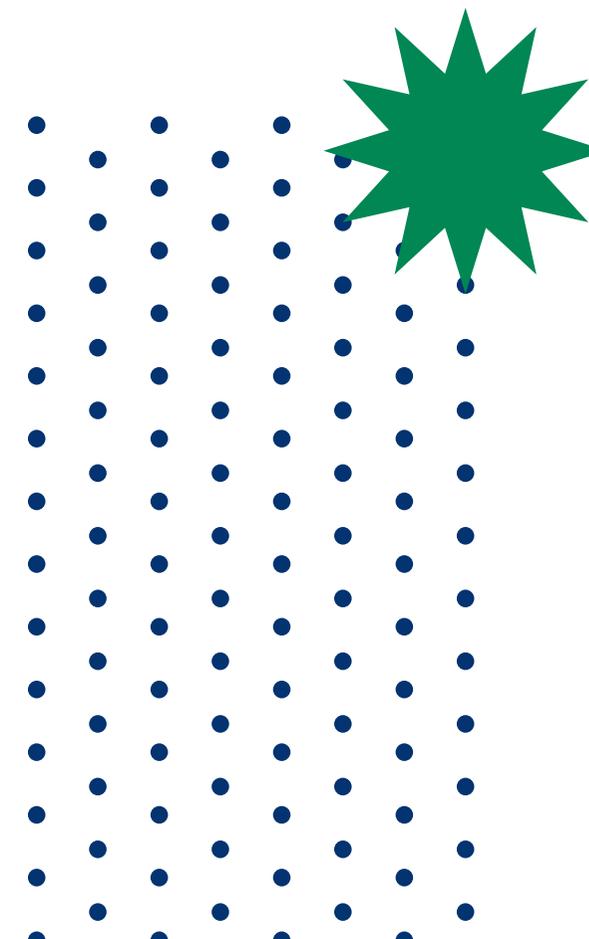
Imaginez que votre propriété intellectuelle fasse l'objet d'une attaque. Résultats de recherche, designs de produits, code source, plans industriels, découvertes scientifiques... toutes ces données non structurées constituent votre capital le plus précieux. Si elles venaient à être compromises, vous perdriez alors des années de travail, votre avantage concurrentiel et des savoirs irremplaçables.

D'où la nécessité de protéger l'intégralité de cette data. Seulement voilà, le défi est immense. En plus d'être colossale, la masse de données non structurées est aussi extrêmement fragmentée et éparpillée entre différents systèmes et lieux de stockage (stockage NAS on-prem, object stores, etc.), ce qui en complique sérieusement le suivi si tout est fait manuellement.

Jusqu'à présent, les entreprises s'en sont remises à des solutions de sauvegarde traditionnelles pour tenter de protéger leurs données non structurées. Le problème c'est que ces méthodes n'offrent ni le contrôle, ni la rapidité, ni la visibilité nécessaires pour mener cette mission à bien.



Selon le cabinet d'études IDC, ces données non structurées représentent aujourd'hui 90 % de la datasphère mondiale.



¹ IDC : The Untapped Value of Unstructured Data, <https://www.box.com/resources/unstructured-data-paper>

Illustration :



Les solutions traditionnelles de sauvegarde n'ont pas été pensées pour de très larges datasets. Sauvegarder des pétaoctets de données avec des outils d'ancienne génération peut prendre des semaines. Et quand bien même ces sauvegardes s'opèreraient rapidement, le processus peut créer des problèmes de latence ou de performance dans l'environnement de production. Des freins qui peuvent conduire les équipes à laisser leurs données sans protection.



Les anciennes solutions de sauvegarde sont dépourvues de visibilité multiplateforme, ce qui vous prive d'une vue unifiée sur vos différents types de stockage. Cette fragmentation constitue un obstacle majeur à la protection d'un volume de données non structurées aussi vaste que protéiforme.



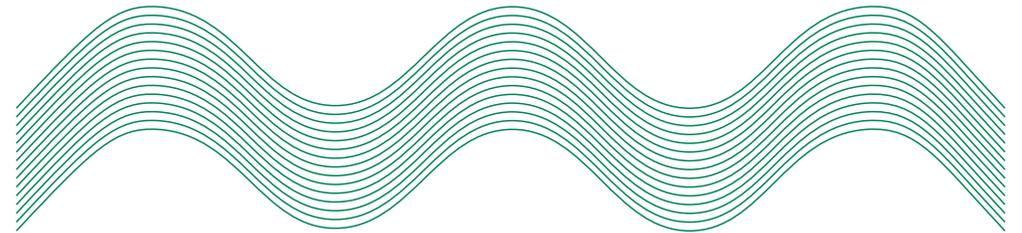
Les solutions classiques de sauvegarde ne vous informent ni sur la localisation de vos données sensibles, ni sur les personnes qui y ont accès. Dans ces conditions, difficile d'identifier les risques et de respecter vos obligations réglementaires.



Les outils traditionnels de sauvegarde ne disposent pas des contrôles de sécurité nécessaires pour lutter contre les ransomwares et autres menaces émergentes.



Avec les méthodes de sauvegarde d'ancienne génération, la restauration des fichiers et dossiers s'opère manuellement, ce qui peut prendre du temps et vous empêcher de respecter vos SLA.



Verdict : face à la prolifération des données non structurées, le maintien de solutions obsolètes de sauvegarde vous mènera tout droit au désastre. Pour vous guider, découvrez les cinq avantages d'une solution moderne de protection des données non structurées pour réduire les risques, renforcer la résilience de vos données et assurer la continuité de votre activité en cas d'attaque.

LES CINQ INDISPENSABLES

D'UNE SOLUTION DE PROTECTION DES DONNÉES NON STRUCTURÉES

1 Conjuguer protection et performance sur des pétaoctets de données non structurées

Immanquablement, les anciens systèmes de sauvegarde commencent à saturer dès lors que le volume de données non structurées atteint le seuil du pétaoctet. La raison est simple : ces outils n'ont pas été conçus pour répondre au volume et au débit colossaux qu'exige la protection de milliards de fichiers.

Face à la quantité astronomique de données, les solutions d'ancienne génération montrent des signes de faiblesse. Les performances commencent à ralentir, non seulement au sein de la solution de sauvegarde, mais aussi du côté des systèmes à sauvegarder. Vos objectifs de point de restauration (RPO) s'éloignent peu à peu, tandis que vos fenêtres de sauvegarde s'allongent et que le risque augmente sur vos informations critiques. Néanmoins, ce n'est pas en investissant dans des solutions matérielles que vous réglerez le problème. Ce parti pris est aussi vain que coûteux. À l'image du NDMP (Network Data Management Protocol), les approches classiques n'ont ni la scalabilité, ni la capacité de reconnaissance des applications nécessaires pour gérer de telles quantités de données. Et ce n'est pas l'ajout d'instances matérielles qui pourra combler ces lacunes.

La solution ? Une approche moderne capable de protéger des milliards de fichiers avec des fonctions d'analyse, d'indexation et de transfert des données hautement synchronisées. En maximisant le débit et en limitant la bande passante de façon dynamique pour une utilisation optimale du réseau, vous pouvez raccourcir vos fenêtres de sauvegarde et assurer une protection complète de vos données, et ce, sans exploser vos budgets.



CONSEIL

Pour une sauvegarde haute-performance, privilégiez les solutions de protection des données non structurées offrant un streaming parallèle et une qualité de service (QoS) dynamique. Ces outils sécurisent des pétaoctets de données avec une telle efficacité qu'ils n'impactent nullement les workloads de production.

2

Visibilité à 360° sur l'ensemble de vos données non structurées

Nous avons déjà mentionné comment, en raison de l'éparpillement des données non structurées dans une multitude d'emplacements et de plateformes NAS, il était difficile de les localiser précisément, d'identifier qui y accède et de s'assurer de leur protection.

Or, côté visibilité et sécurisation, les solutions de sauvegarde d'ancienne génération restent loin du compte. En cause : des architectures cloisonnées qui exigent une supervision, des politiques et des plannings spécifiques, incompatibles avec l'application d'une stratégie de protection des données homogène et garantie par SLA. Autre inconvénient de ces silos, la difficulté d'obtenir une vue complète de l'ensemble de vos données non structurées. Croissance des données, schémas d'utilisation, tendances... tout manque de visibilité centralisée dans ces domaines entrave la gestion du cycle de vie des données et fragilise les décisions quant aux données à archiver. Dans le cas de sauvegardes dans le cloud, le stockage de vastes quantités de données dans la mauvaise classe pourrait considérablement alourdir la facture du CSP.

Le moment est donc venu de miser sur une approche unifiée qui, via une console unique, vous offrira la vue globale nécessaire pour reprendre le contrôle de vos données non structurées. Les tableaux de bord centralisés ont le double avantage d'apporter des éclairages actionnables pour une gestion proactive des données et de favoriser l'application homogène des politiques.



CONSEIL

Misez sur des solutions dotées d'une console unifiée pour protéger vos données non structurées dans l'ensemble des sites et systèmes NAS. Cette visibilité complète et centralisée est indispensable à une gestion optimisée du cycle de vie des données et au respect des obligations réglementaires.

3

Une détection des anomalies garante de la sécurité des données à grande échelle

Aujourd'hui, les cybercriminels affûtent leurs méthodes pour cibler vos données d'entreprise. Pour preuve, 93 % des organisations victimes d'une attaque ont signalé des actions visant spécifiquement leurs données de sauvegarde. Dans 73 % de ces cas, les attaquants sont parvenus plus ou moins à leurs fins².

Le problème s'explique en partie par la tendance des solutions traditionnelles à laisser vos données de sauvegarde en ligne, à la portée de tous, sans mettre en place des air gaps logiques robustes.

L'air gap établit une séparation logique qui isole et dissimule vos sauvegardes pour les tenir à l'abri des menaces. Sans ce type de solutions, vos sauvegardes sont à la merci des acteurs cyber et peuvent compromettre vos capacités de restauration si elles venaient à tomber entre de mauvaises mains.

Raison de plus pour recourir à des **sauvegardes immuables**, à savoir des sauvegardes que l'on ne peut ni modifier, ni effacer, ni changer. Seulement voilà, cette fonctionnalité figure rarement dans les solutions d'ancienne génération. Faute d'immutabilité, vos sauvegardes peuvent être écrasées en cas d'attaque, vous privant ainsi d'un point de restauration sûr.

Autre point faible des outils de sauvegarde classiques, leurs **contrôles des accès basés sur les rôles (RBAC)**

restent rudimentaires, sans parler de leurs autorisations trop permissives. Cette sécurité lacunaire laisse donc la porte ouverte à des activités interne malveillantes ou au vol d'identifiants par des hackers. Sans contrôles granulaires d'accès basé sur les rôles, il est impossible d'appliquer le principe du moindre privilège. Conséquence : les utilisateurs (ou des cybercriminels munis d'identifiants volés) peuvent accéder à plus de données que nécessaire, ce qui accroît fortement la surface de risque.

En ce sens, votre nouvelle solution de protection des données non structurées devra intégrer des contrôles de sécurité et tout un éventail de fonctionnalités : Air gap, immutabilité des sauvegardes, RBAC, sans oublier **la détection des anomalies**.

La fonction de détection des anomalies vous guide dans votre investigation des ransomwares et vous aide à cerner l'ampleur de l'attaque en repérant les données supprimées, modifiées et cryptées. Ces précieuses informations vous permettront de restaurer très précisément les données dont vous avez besoin, au lieu de lancer un (long) processus de restauration à grande échelle. Résultat, vous pourrez reprendre votre activité plus vite avec, de surcroît, des données intactes.



CONSEIL

Priorisez les solutions de protection des données non structurées embarquant ces quatre fonctionnalités indispensables : air gaps logiques robustes, sauvegardes immuables, contrôles granulaires des accès basés sur les rôles et détection des anomalies. Ces différentes couches de sécurité agissent en synergie pour mettre vos données de sauvegarde à l'abri des accès non autorisés et des tentatives d'altération. Et en cas d'attaque, elles facilitent la reprise des activités.

4

Visibilité et classification des données sensibles

Par données sensibles, on entend tout type d'information qui, en cas de compromission, pourrait porter préjudice à des personnes ou des entreprises. Cela inclut les données à caractère personnel (DCP), les données financières, la propriété intellectuelle, les dossiers médicaux ou tout type de renseignement devant être protégé à des fins de confidentialité, sécurité et conformité.

La gouvernance et la sécurité des données sensibles figurent donc en tête des priorités pour respecter les exigences réglementaires et conserver la confiance des clients. Cependant, à l'heure où les données non structurées se comptent en pétaoctets, la localisation et l'identification des données sensibles ou réglementées prennent des allures de mission impossible.

Les anciens outils de sauvegarde sont totalement dépourvus de capacités de découverte et de classification des données. Sans informations sur le type et l'emplacement des données sensibles en votre possession, votre posture de sécurité et de conformité comporte de dangereux angles morts.

Car faute de pouvoir identifier des données sensibles (données de santé, de paiement ou à caractère personnel) dans vos datasets,

vous risquez d'exposer involontairement ces informations ou d'enfreindre les réglementations sur la confidentialité (RGPD, HIPPA, CCPA, etc.). La mise en place de protections adaptées passe donc par une localisation de vos données critiques.

Par ailleurs, ce manque de visibilité peut conduire à une surutilisation des ressources de sauvegarde, synonyme de hausse des coûts. Sans idée précise du niveau de sensibilité et de la valeur de vos données, vous êtes contraint d'appliquer à toutes le même traitement. Le problème, c'est que la sauvegarde et la réplication d'informations non critiques finiront par faire exploser vos coûts de stockage.

C'est là que les solutions conjuguant protection des données et analyse approfondie des contenus entrent en jeu. Leur mission est double : réduire l'exposition des données sensibles et simplifier la mise en conformité. Ainsi, la découverte, la classification et le reporting automatiques des données sensibles vous permettent de protéger en priorité vos données les plus stratégiques, de classer vos données en fonction des risques et, au final, de mieux maîtriser les coûts.



CONSEIL

Choisissez une solution de protection équipée de fonctions de découverte et de classification des données sensibles. Grâce à l'identification des données réglementées et l'évaluation des risques en matière de confidentialité et de sécurité, vous aurez toutes les cartes en main pour renforcer la gouvernance des données et prouver votre conformité. Cet inventaire précis des données en votre possession vous permettra aussi de mieux protéger votre capital le plus précieux et de ne sauvegarder que le strict nécessaire.

5

Restauration granulaire et efficace des données

Dans une enquête réalisée en 2024 sur le coût horaire des interruptions de service, le cabinet Information Technology Intelligence Consulting (ITIC) a révélé que le coût moyen d'une seule heure d'interruption dépasse désormais 300 000 \$ pour plus de 90 % des grandes entreprises et ETI³. En cas d'incident, chaque seconde compte. Plus vous pourrez restaurer vos données rapidement et précisément, plus vous limiterez les dégâts. Ce qui paraît mal engagé si vous recourez encore à des solutions d'ancienne génération.

L'exercice s'apparenterait même à chercher une aiguille dans une botte de foin. Sans fonctionnalités de recherche granulaires, les administrateurs IT se retrouvent à devoir passer au crible des tonnes de données éparpillées dans l'ensemble de l'environnement pour tenter de dresser un bilan des contenus touchés par l'attaque.

Faute de pouvoir identifier les données compromises, ils n'ont d'autre choix que de restaurer les systèmes dans leur intégralité. Avec pour conséquences l'encombrement du réseau, la saturation des équipements de stockage et, *in fine*, le ralentissement de la restauration. Toutefois,

une question essentielle subsiste... les données en cours de restauration sont-elles vraiment saines ?

C'est là un autre point faible des solutions d'ancienne génération : l'impossibilité de vérifier l'intégrité des sauvegardes. Concrètement, vous pourriez restaurer à votre insu des données corrompues ou infectées. Non seulement vous voilà de retour au point de départ mais, pire encore, vous avez gaspillé énormément de temps et de ressources. Du reste, ces outils traditionnels sont souvent dépourvus de fonctions de restauration automatique, ce qui ralentit davantage le processus.

Pour réduire les pertes de données et accélérer la reprise d'activité, il vous faut donc une solution garante d'une restauration ciblée et rapide à grande échelle. Ses capacités de recherche approfondie et de récupération granulaire vous permettront de restaurer les données requises sans délai. Quant à la vérification des sauvegardes et aux workflows de restauration automatique, ils accéléreront le processus de A à Z.

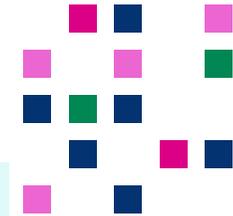


CONSEIL

Optez pour des outils garants d'une récupération rapide et ciblée à grande échelle. L'objectif : localiser et récupérer promptement des données spécifiques sans avoir à restaurer l'intégralité des systèmes. De plus, veillez à ajouter la vérification et l'automatisation des sauvegardes à votre cahier des charges. Ces options s'avèreront utiles pour simplifier le processus de restauration, réduire les erreurs humaines et gagner en efficacité.

3 Rapport ITIC 2024 sur le coût horaire des interruptions de service, 1^{re} partie, <https://itic-corp.com/itic-2024-hourly-cost-of-downtime-report/>

MODERNISEZ VOTRE PROTECTION DES DONNÉES NON STRUCTURÉES



Les anciennes solutions de sauvegarde ont fait leurs temps. Face à l'évolution du champ des menaces et de la data, l'heure est venue de tourner la page. Aujourd'hui, les données non structurées exigent une protection et une gestion rigoureuses au même titre que les autres données critiques.

Pour lever ces obstacles, il est impératif de miser sur une solution conçue pour traiter des données non structurées à l'échelle du pétaoctet. C'est là que Rubrik NAS Cloud Direct intervient pour vous aider à renforcer la protection de votre capital le plus précieux.

Découvrez comment Rubrik NAS Cloud Direct comble les lacunes d'une protection classique des données non structurées :



Sauvegarde rapide et performances à grande échelle

Rubrik NAS Cloud Direct sauvegarde et restaure des pétaoctets de données et des milliards de fichiers avec une rapidité et une efficacité bien supérieures au NDMP, surclassant de loin les approches traditionnelles. Les capacités d'analyse, d'indexation et de transfert hautement parallèles des données maximisent le débit, tandis que la fonction QoS intelligente élimine toute répercussion sur les workloads de production.



Configuration facile, sauvegardes ultrarapides et procédures de restauration simplissimes.

Administrateur infrastructure IT senior
Entreprise du secteur des loisirs et du divertissement



Gestion et visibilité unifiées

Notre solution NAS Cloud Direct est équipée d'une console centralisée pour une gestion unifiée des données non structurées. Ses tableaux de bord complets vous offrent des rapports et éclairages actionnables pour optimiser la protection, l'archivage et la conformité. Vos opérations gagnent en simplicité grâce à l'application homogène de politiques pour l'ensemble de vos données.



L'adoption de Rubrik NAS Cloud Direct a amélioré notre efficacité en termes de rapidité et de résultats.

Responsable conception produit
Établissement financier





Sécurité avancée des données avec Anomaly Detection

Rubrik NAS Cloud Direct s'appuie sur des air gaps logiques, des sauvegardes immuables et des contrôles d'accès basés sur les rôles pour renforcer la sécurité des données. La fonction Anomaly Detection de Rubrik vous prévient en cas de problème et vous permet d'évaluer l'impact potentiel d'un incident. Visualisation du déroulé de l'attaque, identification des activités malveillantes, accélération de la réponse et de la reprise... Rubrik vous accompagne à chaque étape.

“

Nous pouvons désormais surveiller et analyser nos sauvegardes NAS. La moindre anomalie nous est signalée, ce qui nous permet d'investiguer sur le champ.

Kevin Mortimer

Responsable des opérations, University of Reading

”



Monitoring des données sensibles et conformité

La solution NAS Cloud Direct combine protection des données et analyse des contenus pour découvrir, classer et générer des rapports sur les données sensibles. Détectez automatiquement les informations personnelles, médicales, bancaires et autres données réglementées pour évaluer les risques de non-conformité et protéger facilement votre capital data le plus précieux.

“

NAS Cloud Direct surveille les systèmes et me prévient en cas de problème. J'ai enfin retrouvé le sommeil.

Travis Spurley

Ingénieur système senior, Quantum Spatial

”



Récupération rapide et granulaire à grande échelle

Pour minimiser la perte de données et les interruptions, Rubrik NAS Cloud Direct assure une recherche instantanée et une récupération granulaire des données impactées. Ainsi, en cas d'attaque, notre solution inspecte des milliards de fichiers en un rien de temps et orchestre la restauration pour vous aider à reprendre vos activités au plus vite.

“

Sa capacité à passer au crible des millions, voire des milliards de fichiers est phénoménale. Sans conteste, la solution Rubrik nous permet de mieux travailler.

Carl Lucas

VP de l'informatique, Quantum Spatial

”



Vos données non structurées sont trop précieuses pour les laisser sous la protection lacunaire de solutions de sauvegarde obsolètes. Miser sur Rubrik, c'est choisir une solution efficace pour protéger et gérer des volumes astronomiques de données non structurées, tout en garantissant votre résilience face à des menaces en constante mutation.



La modernisation des sauvegardes, c'est maintenant.

Découvrez tout ce qu'il faut savoir sur [Rubrik](#) et [NAS Cloud Direct](#).

